(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2004-528616
(P2004-528616A)
(43)公表日　平成16年9月16日(2004.9.16)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F 12/14	320F	5B017
H04L 9/08	H04L 9/00	601A	5J104

審査請求 未請求　予備審査請求 有　（全 72 頁）

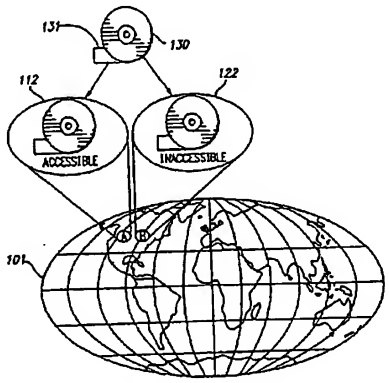
(21)出願番号	特願2002-539934(P2002-539934)
(86)(22)出願日	平成13年10月30日(2001.10.30)
(85)翻訳文提出日	平成15年4月30日(2003.4.30)
(86)国際出願番号	PCT/US2001/048076
(87)国際公開番号	WO2002/037246
(87)国際公開日	平成14年5月10日(2002.5.10)
(31)優先権主張番号	09/699,832
(32)優先日	平成12年10月30日(2000.10.30)
(33)優先権主張国	米国(US)

(71)出願人　503161028
ゲオコデックス・エルエルシー
アメリカ合衆国、カリフォルニア州　９１４３６－１７６３、エンシーノ、スイート３０１、ベントゥーラ・ブールバード　１６８６１
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊

最終頁に続く

(54)【発明の名称】位置識別属性を使用してデジタル情報へのアクセスを制御するためのシステムおよび方法

(57)【要約】
デジタル情報へのアクセスを制御するための方法および装置は特定の地理的な位置を規定する位置識別属性を使用する。位置識別属性はその特定の地理的な位置でのみデジタル情報がアクセスされることができるようにこのデジタル情報に関連付けられている。位置識別属性はさらに位置値と近接値とを含んでいる。位置値はデジタル情報の予定された受信アプライアンスの位置に対応し、緯度、経度および高度のディメンションに関してさらに規定されることができる。位置識別属性は特定の地理的な位置でのみデジタル情報にアクセスすることを可能にすることによって実施される。この実施手順の第１の部分としてデジタル情報へのアクセスが試みられたアプライアンスの位置が識別される。その後このアプライアンス位置は位置識別属性によって規定された特定の地理的位置と比較され、そのアプライアンス位置が特定の地理的位置の範囲内に入っている場合にのみデジタル情報へのアクセスが許される。アプライアンスの位置を識別する多くの方法が存在し、（１）アプライアンスの街路アドレスからのアプライアンスの位置の決定、（２）アプ



【特許請求の範囲】
【請求項１】
少なくとも特定の地理的位置を規定する位置識別属性をデジタル情報に関連付けるステップを含んでおり、前記デジタル情報は前記特定の地理的位置においてのみアクセスされることができるデジタル情報へのアクセスを制御する方法。
【請求項２】
前記関連付けるステップは、少なくとも位置値および近接値を含むように前記位置識別属性を生成するステップをさらに含んでいる請求項１記載の方法。
【請求項３】
前記位置値は、前記デジタル情報の意図された受信アプライアンスの位置に対応している請求項２記載の方法。
【請求項４】
時間値を含むように前記位置識別属性を生成するステップをさらに含んでいる請求項２記載の方法。
【請求項５】
前記位置値には、緯度および経度のディメンションがさらに含まれている請求項２記載の方法。
【請求項６】
前記位置値には、高度のディメンションがさらに含まれている請求項５記載の方法。
【請求項７】
前記近接値は、前記位置を囲むゾーンに対応している請求項３記載の方法。
【請求項８】
方形領域、多角形領域、円形領域および楕円形領域からなるグループから前記ゾーンを選択するステップをさらに含んでいる請求項７記載の方法。
【請求項９】
郵便番号、州、市、郡、電話地域コードおよび国の少なくとも１つを含む既知の地理的領域から前記ゾーンを選択するステップをさらに含んでいる請求項７記載の方法。
【請求項１０】
前記特定の地理的位置においてのみ前記デジタル情報へのアクセスを可能にすることにより前記位置識別属性を実施するステップをさらに含んでいる請求項１記載の方法。
【請求項１１】
前記実施するステップは、前記デジタル情報へのアクセスが試みられたアプライアンスの位置を識別するステップをさらに含んでいる請求項１０記載の方法。
【請求項１２】
前記実施するステップは、前記位置識別属性により規定された前記特定の地理的位置と前記アプライアンスの位置を比較し、前記アプライアンスの位置が前記特定の地理的位置の範囲に入っている場合にのみ前記デジタル情報へのアクセスを可能にするステップをさらに含んでいる請求項１１記載の方法。
【請求項１３】
前記位置を識別するステップは、前記アプライアンスの街路アドレスから前記アプライアンスの位置を決定するステップをさらに含んでいる請求項１１記載の方法。
【請求項１４】
前記位置を識別するステップは、前記アプライアンス中に記憶されているファイルから前記アプライアンス位置を検索するステップをさらに含んでいる請求項１１記載の方法。
【請求項１５】
前記位置を識別するステップは、前記アプライアンスに内蔵されたＧＰＳ受信機から前記アプライアンス位置を復元するステップをさらに含んでいる請求項１１記載の方法。
【請求項１６】
前記位置を識別するステップは、前記アプライアンスにより受信されたＲＦ信号を三角法で測定することによって前記アプライアンス位置を復元するステップをさらに含んでいる

請求項１１記載の方法。
【請求項１７】
前記関連付けるステップは、少なくとも部分的に前記位置識別属性に基づいた暗号化キーを使用して前記デジタル情報を暗号化するステップをさらに含んでいる請求項１記載の方法。
【請求項１８】
前記生成するステップは、前記特定の地理的位置を囲む領域を規定するエリアパラメータを生成し、前記暗号化キーを生成するために前記エリアパラメータを前記位置識別属性と決定論的に組合せるステップをさらに含んでいる請求項１７記載の方法。
【請求項１９】
前記特定の地理的位置においてのみ前記デジタル情報の暗号解読を可能にすることにより前記位置識別属性を実施するステップをさらに含んでいる請求項１７記載の方法。
【請求項２０】
前記実施するステップは、少なくとも部分的に前記特定の地理的位置に基づいて、前記デジタル情報を暗号解読するために使用される解読キーを生成するステップをさらに含んでいる請求項１９記載の方法。
【請求項２１】
前記関連付けるステップは、前記位置識別属性を前記デジタル情報と統合するステップをさらに含んでいる請求項１記載の方法。
【請求項２２】
前記デジタル情報を含むファイルの一部分の中に前記位置識別属性を含ませるステップをさらに含んでいる請求項２１記載の方法。
【請求項２３】
前記特定の地理的位置においてのみ対応したソフトウェアアプリケーションによる前記ファイルへのアクセスを可能にすることにより前記位置識別属性を実施するステップをさらに含んでいる請求項２２記載の方法。
【請求項２４】
前記特定の地理的位置においてのみメモリからの前記デジタル情報の検索を可能にすることにより前記位置識別属性を実施するステップをさらに含んでいる請求項１記載の方法。
【請求項２５】
前記特定の地理的位置においてのみ前記デジタル情報の視覚的表示を可能にすることにより前記位置識別属性を実施するステップをさらに含んでいる請求項１記載の方法。
【請求項２６】
ＣＤ－ＲＯＭ、ＤＶＤ、ディスケット、ビデオカセットおよびテープの少なくとも１つを含む固定したフォーマットで前記デジタル情報および前記位置識別属性を記憶するステップをさらに含んでいる請求項１記載の方法。
【請求項２７】
電話線、ビデオケーブル、衛星放送、光ファイバ、および無線の少なくとも１つによって電子的な形態で前記デジタル情報および前記位置識別属性を送信するステップをさらに含んでいる請求項１記載の方法。
【請求項２８】
メモリを有するプロセッサを具備し、
このメモリは、少なくとも特定の地理的位置を規定する位置識別属性とデジタル情報との関連付けをプロセッサに行わせるように動作可能なソフトウェア命令を記憶するように構成され、
前記デジタル情報は前記特定の地理的位置においてのみアクセス可能であるデジタル情報へのアクセスを制御するための装置。
【請求項２９】
前記位置識別属性はさらに少なくとも位置値および近接値を含んでいる請求項２８記載の装置。

【請求項３０】
前記位置値は、前記デジタル情報の意図された受信アプライアンスの位置に対応している請求項２９記載の装置。
【請求項３１】
前記位置識別属性はさらに時間値を含んでいる請求項２９記載の装置。
【請求項３２】
前記位置値には、緯度および経度のディメンションがさらに含まれている請求項２９記載の装置。
【請求項３３】
前記位置値には、高度のディメンションがさらに含まれている請求項３２記載の装置。
【請求項３４】
前記近接値は、前記位置を囲むゾーンに対応している請求項２９記載の装置。
【請求項３５】
前記ゾーンにはさらに、方形領域、多角形領域、円形領域および楕円形領域の少なくとも１つがさらに含まれている請求項３４記載の装置。
【請求項３６】
前記ゾーンには、郵便番号、州、市、郡、電話地域コードおよび国の１つを含む既知の地理的領域が含まれている請求項３２記載の装置。
【請求項３７】
前記特定の地理的位置においてのみ前記デジタル情報へのアクセスを可能にすることにより前記位置識別属性を実施する手段をさらに含んでいる請求項２８記載の装置。
【請求項３８】
前記実施する手段は、前記デジタル情報へのアクセスが試みられたアプライアンスの位置を識別する手段をさらに含んでいる請求項３７記載の装置。
【請求項３９】
前記実施する手段は、前記位置識別属性により規定された前記特定の地理的位置と前記アプライアンスの位置を比較する手段をさらに含んでおり、前記アプライアンスの位置が前記特定の地理的位置の範囲に入っている場合にのみ前記デジタル情報へのアクセスが可能にされる請求項３８記載の装置。
【請求項４０】
前記位置識別する手段は、前記アプライアンスに対する街路アドレスから前記アプライアンスの位置を決定する手段をさらに含んでいる請求項３８記載の装置。
【請求項４１】
前記位置識別する手段は、前記アプライアンス中に記憶されているファイルから前記アプライアンス位置を検索する手段をさらに含んでいる請求項３８記載の装置。
【請求項４２】
前記位置識別する手段は、前記アプライアンスに内蔵されたＧＰＳ受信機から前記アプライアンス位置を復元する手段をさらに含んでいる請求項３８記載の装置。
【請求項４３】
前記位置識別する手段は、前記アプライアンスにより受信されたＲＦ信号を三角法で測定することによって前記アプライアンス位置を復元する手段をさらに含んでいる請求項３８記載の装置。
【請求項４４】
前記メモリはさらに、少なくとも部分的に前記位置識別属性に基づいた暗号化キーを使用して前記デジタル情報を前記プロセッサに暗号化させるように動作することのできるソフトウェア命令を記憶している請求項２８記載の装置。
【請求項４５】
前記特定の地理的位置を囲む領域を規定するエリアパラメータをさらに含んでおり、前記メモリはさらに、前記暗号化キーを生成するために前記エリアパラメータと前記位置識別属性との決定論的な組合せを前記プロセッサに行わせるように動作可能なソフトウェア命

令を記憶している請求項４４記載の装置。
【請求項４６】
前記特定の地理的位置においてのみ前記デジタル情報の暗号解読を可能にすることにより前記位置識別属性を実施する手段をさらに含んでいる請求項４４記載の装置。
【請求項４７】
前記実施する手段は、少なくとも部分的に前記特定の地理的位置に基づいて、前記デジタル情報を暗号解読するために使用される解読キーを生成する手段をさらに含んでいる請求項４６記載の装置。
【請求項４８】
前記位置識別属性は前記デジタル情報と統合される請求項２８記載の装置。
【請求項４９】
前記位置識別属性は、前記デジタル情報を含むファイルの一部分の中に含まれている請求項４８記載の装置。
【請求項５０】
前記特定の地理的位置においてのみ対応したソフトウェアアプリケーションによる前記ファイルへのアクセスを可能にすることにより前記位置識別属性を実施する手段をさらに含んでいる請求項４９記載の装置。
【請求項５１】
前記特定の地理的位置においてのみメモリからの前記デジタル情報の検索を可能にすることにより前記位置識別属性を実施する手段をさらに含んでいる請求項２８記載の装置。
【請求項５２】
前記特定の地理的位置においてのみ前記デジタル情報の視覚的表示を可能にすることにより前記位置識別属性を実施する手段をさらに含んでいる請求項２８記載の装置。
【請求項５３】
前記デジタル情報および前記位置識別属性は、ＣＤ－ＲＯＭ、ＤＶＤ、ディスケット、ビデオカセットおよびテープの１つを含む固定したフォーマットで配置されている請求項２８記載の装置。
【請求項５４】
前記デジタル情報および前記位置識別属性は、電話線、ビデオケーブル、衛星放送、光ファイバ、および無線の１つによって電子的な形態で送信される請求項２８記載の装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、デジタル情報の伝達に関し、とくに、デジタル情報と関連付けられた位置完全性属性を使用してデジタル情報の交換を制御するための方法およびシステムに関する。
【０００２】
【従来の技術】
コンピュータ、通信およびネットワークテクノロジーの急速な進歩により、数年前には不可能だった新しい機会やアプリケーションがどっと雪崩のように可能になってきている。これらの進歩は、インターネット人気の爆発的な上昇によって例証される。技術的に知られているように、インターネットは、全種類のコンピュータが互いに通信し、情報を共用することを可能にするコンピュータネットワークの相互接続である。あらゆる規模の企業、個人、政府機関、慈善団体および学術センターがインターネットを常に使用して情報を共用し、サービスを配信し、広範囲にわたるコンテンツを交換している。インターネットは、何れの機関からも制御されず管理もされないシステムの分布形ネットワークとして機能する。情報の交換を容易にする物理的および論理的通路がこれらのネットワークを互いに結び付けている。
【０００３】
こ情報アクセスが社会にもたらされたことには非常に高い価値があるにもかかわらず、制御されていない情報フローに関連した費用もまた著しい額である。通信システムに関する

最も重要な考慮事項の１つは、情報セキュリティおよびアクセスに対する制御である。多くの場合、情報の送信者は、意図した受信者だけがその情報にアクセスできると共に意図しない任意の他の受信者がアクセスを拒否されることを確実にしたいと希望する。この情報セキュリティおよびアクセス制御は典型的に、公衆ネットワークによる送信のために情報を秘密コードに変換する暗号化システムによって行われる。この暗号化システムでは、送信者が暗号アルゴリズムを使用して元のデータ、すなわち“平文”を“暗号文”と呼ばれる符号化された等価なものに変換する。その後、暗号文は受信者によって復号（または解読）され、それによって平文に戻されることができる。暗号アルゴリズムは、その長さが典型的に４０乃至１２８ビットの２進数であるキーを使用する。キーの中のビット数が大きくなると、キーの組合せの可能性がそれだけ一層多くなり、したがってそのコードを解くのに要する時間が長くなる。データは、キーの中のビットとデータビットとを数学的に組合せることによって暗号化されるか、あるいは“ロック”される。受信端において、そのキーはそのコードを“ロック解除”し、元のデータを復元するために使用される。

【０００４】

一般的には、２つの暗号化方法が使用されている。第１の方法は、平文の暗号化および解読を行うために送信者および受信者の両者によって使用される秘密キーを使用する。この方法の欠点は、送信者が秘密キーを機密解除の危険にさらさずに受信者に伝送することが困難なことである。第２の方法は、公開キー暗号化として知られており、この暗号化は秘密キーおよび公開キーとして知られている２つのキーを使用する。各パーティは、秘密を保持されて共有されない秘密キーと、公に利用可能にされている公開キーとを有している。公開キーは平文情報を暗号化するために使用され、秘密キーは暗号文メッセージを解読するために使用される。秘密キーは、公開キーから数学的に導出されてはならない。通信を行っているパーティは、インターネットのような機密保護されていない通信チャンネルによって彼等の公開キーを交換し、その後彼等のメッセージを暗号化するために公開キーを使用してもよい。その後、受信者はそのメッセージを解読するために秘密キーを使用する。

【０００５】

通信システムに対する別の重要な考慮事項は、著作権保護されたデジタルコンテンツの無許可コピーの防止である。通常の計算および通信システムに関して、良心を欠いた者はデジタル形態の著作権のある作品（たとえば、音楽、著作物、写真、ビデオ、ソフトウェア等）の同一コピーを無数に容易に作成して分配することができる。さらに、商業的に利用可能なファイル指標付けサービスにより、コンピュータユーザは別のユーザのコンピュータシステム上のデジタルファイルの位置を突き止め、それにアクセスすることが容易に可能となり、それによって広範囲に及ぶ著作権侵害の可能性が著しく増加する。Ｎａｐｓｔｅｒ社（Ｓａｎ Ｍａｔｅｏ，ＣＡ）によって提供されている１つのこのようなサービスは、現在インターネットにログオンされている別のコンピュータ上に存在する人気のＭＰ３フォーマットの音楽ファイルの位置を突き止めるようにＮａｐｓｔｅｒウェブサイトと共同して動作するファイル共用アプリケーションを提供する。グヌーテラ（Ｇｎｕｔｅｌｌａ）として知られている同様にサービスは、種々の情報が世界全体で利用可能なものにするユーザおよび組織のゆるやかな自由な連合体であるグヌーテラ・ネット上のソフトウェアおよびドキュメントをユーザがサーチすることを可能にするファイル共用システムを提供する。音楽ファイル用に調整され、中央化されたリスティングを与えるナプスター（Ｎａｐｓｔｅｒ）とはグヌーテラは異なり、グヌーテラ・ネットは、全ての種類のファイルを含むピア・ツー・ピアネットワークである。これらのファイル共用システムはまた、著作権保護されていないファイルをユーザが共用することを可能にする際はその目的は合法的なものであるが、それらはまた著作権法に違反して著作権保護されたファイルを入手するために広く使用されている。これらのファイル共用システムの違法使用は、著作権の所有者に対する深刻な脅威を表す。

【０００６】

インターネットの積極的な保安管理は、著作権保有者にとって有効なソリューションでは

ない。インターネットの著作権侵害の広範囲で匿名の性質を仮定すると、このような管理努力は論理的に困難である。さらに、インターネット上で交換される情報コンテンツは自由でなければならないという世論のために、大規模な保安管理努力は公的関係の観点から魅力のないものになる。この問題を解決するために、予防措置に焦点を合わせることによって配布されるデジタルコンテンツの著作権を保護する種々のデジタル権利管理（ＤＲＭ）システムが生成されてきた。たとえば、Ｓｅｃｕｒｅ Ｄｉｇｉｔａｌ Ｍｕｓｉｃ Ｉｎｉｔｉａｔｉｖｅ（ＳＤＭＩ）として知られているレコーディング産業向けに提案されたＤＲＭシステムは、デジタル音楽をインターネットによって安全に配布するための１組のルールを明らかにしている。ＳＤＭＡは、ソフトウェアおよびハードウェアのプレーヤがマテリアル（ｍａｔｅｒｉａｌ）を再生するためにサポートしなければならないコンテナフォーマットを含むコンプライアントなＤＲＭシステムを開発するためのガイドラインを提供している。ＳＤＭＩは米国レコーディング産業協会（ＲＩＡＡ）ならびにソニー、ワーナー、ＢＭＧ、ＥＭＩおよびユニバーサルの上位５つの音楽製作会社により支援されることが１９９９年２月に発表された。

【０００７】

これらの努力にもかかわらず、ＤＲＭシステムはいくつかの理由のためにせいぜい不完全なソリューションしか提供しない。第１に、インターネット上で著作権侵害されたコンテンツの利用可能性を仮定すると、通常の売買経路を介してマテリアルのコピーを合法的に購入するよりインターネットによってデジタルファイルを違法にダウンロードするほうが、ユーザにとってはるかに便利で廉価である。違法に入手したマテリアルは合法的にコピーと比較して品質は低いかもしれないが、便利さおよびごく僅かな費用がこの欠点を補償することが多い。

【０００８】

第２に、大部分のＤＲＭテクノロジーは、デジタル情報を保護するためにある形態の暗号化に依存している。非常に実効的であるために、暗号化方式に関する利害関係者は共に暗号化された情報の秘密を保持する利権を有していなければならない。コンテンツの法的購入者はそのコンテンツを見る権利を有しているが、暗号化によって与えられる秘密が確実に保持されるようにする利権は有しない。このために、多くのＤＲＭソリューションにおいて、暗号解読キーをユーザから隠蔽しようと試みるデジタル証明書またはライセンスが使用される。このようなシステムでは、コンテンツの全てのコピーは同じ方法で暗号化され、メディアプレーヤーは解読されたコンテンツを表示するか、あるいは再生するためにユーザの権利の妥当性を検査する。しかしながら、暗号化されたコンテンツおよび暗号解読キーは隠蔽されているにもかかわらず、ユーザはそれにアクセスすることが可能であるため、高度な知識を有するユーザは、ＤＲＭソリューションを逆処理してその暗号化を解読し、それによって解読されたコンテンツを何等妨害を受けずにコピーして配布することができる。これより技術的に劣るが、コンテンツの暗号化されていないコピーを入手する別の方法、たとえば、コンテンツが再生中に合法的に表示されているときにそのデジタルビデオデータファイルの各フレームをビデオテープ撮りする等もまた良心のないユーザは利用することが可能である。

【０００９】

【発明が解決しようとする課題】

したがって、これらおよびその他の欠点を克服したデジタル情報交換の制御方法を提供することが非常に望ましい。とくに、セキュリティおよび情報へのアクセスに対する制御を可能にすると共に著作権保護されたコンテンツの無許可コピーを阻止する情報交換システムおよび方法を提供することが望まれている。

【００１０】

【課題を解決するための手段】

本発明にしたがってデジタル情報へのアクセスを制御するための方法および装置は、特定の地理的な位置を規定する位置識別属性を使用する。この位置識別属性は、その特定の地理的な位置でのみデジタル情報がアクセスされることができるように、このデジタル情報

に関連付けられている。位置識別属性はさらに、位置値と、近接値とを含んでいる。位置値はデジタル情報の予定された受信アプライアンスの位置に対応し、緯度、経度および高度のディメンションに関してさらに規定されることができる。近接値は、その位置を囲むゾーンに対応している。位置識別属性はさらに、特定の地理的な位置でおよび特定の時間期間中にのみデジタル情報がアクセスされることができるように、時間値を含んでいてもよい。

【００１１】

本発明の一般的な実施形態において、デジタル情報へのアクセスは、位置識別属性により規定された特定の地理的位置で行われたもののみが許される。この実施手順の第１の部分として、デジタル情報へのアクセスが求められたアプライアンスの位置が識別される。アプライアンスの位置を識別する多くの方法が存在し、（１）そのアプライアンスの街路アドレスからアプライアンスの位置を決定し、（２）そのアプライアンス中に記憶されているファイルからそのアプライアンス位置を検索し、（３）アプライアンスに内蔵されたＧＰＳ受信機からそのアプライアンス位置を復元し、および（４）そのアプライアンスにより受信されたＲＦ信号を三角法で測定することによってそのアプライアンス位置を復元することが含まれる。アプライアンスが識別された後、それは位置識別属性によって規定された特定の地理的位置と比較される。そのアプライアンス位置が特定の地理的位置の範囲内に入っている場合にのみ、デジタル情報へのアクセスが許される。

【００１２】

上述した一般的な実施形態に基づく本発明のさらに特有の実施形態において、デジタル情報は少なくとも部分的に位置識別属性に基づいた暗号化キーを使用して暗号化される。暗号化キーはさらにエリアパラメータに基づいていてもよく、このエリアパラメータは位置識別属性から決定され、暗号化されたデジタル情報と共に含まれている。エリアパラメータは地理的エリアの形状を記述するが、その地理的エリアがどこに位置しているかは識別しない。エリアパラメータは、暗号化キーを生成するために位置識別属性と決定論的に組合せられる。暗号化されたデジタル情報を受信したアプライアンスは、受信したエリアパラメータと、および上述の方法の任意のものにしたがって決定されたそのアプライアンス位置とに基づいて、そのデジタル情報を暗号解読するための解読キーを生成することができる。そのアプライアンス位置が位置識別属性の近接エリア内に入っていない場合には、アプライアンスはそのデジタル情報を暗号解読するための解読キーを生成することができない。このようにして、特定の地理的位置のみでのデジタル情報の暗号解読を可能にすることにより、位置識別属性が実施される。

【００１３】

上述した一般的な実施形態に基づく本発明の別の特有の実施形態において、位置識別属性は、デジタル情報を含むファイルの一部分の中においてデジタル情報と統合されている。このファイルにアクセスするソフトウェアアプリケーションまたはオペレーティングシステムは、位置識別属性によって規定された特定の地理的位置においてのみそのファイルへのアクセスを可能にすることにより位置識別属性を実施する。

【００１４】

上述した一般的な実施形態に基づく本発明のさらに別の特有の実施形態において、位置識別属性は、ハードディスクコントローラまたはビデオコントローラのようなアプライアンスのハードウェア素子に関連したハードウェア制御装置により実施される。そのハードウェア素子が位置識別属性により規定されたその特定の地理的位置に位置している場合にのみ、デジタル情報はメモリから検索され、あるいはビデオモニタ上に表示されることが可能となる。

【００１５】

以下の本発明の好ましい実施形態の詳細な説明を検討することにより、当業者は位置識別属性を使用してデジタル情報へのアクセスを制御するためのシステムおよび方法をさらに完全に理解すると共に、本発明の別の利点および目的を認識するであろう。この明細書の最後に簡単な説明が示されている添付図面を参照とする。

【００１６】
【発明の実施の形態】
本発明は、セキュリティおよびデジタル情報へのアクセスに対する制御を可能にすると共に著作権保護されたコンテンツの無許可コピーを阻止するデジタル情報交換制御方法に対する必要性を満足させるものである。以下の詳細な説明において、１以上の図面に示されている同じ素子を表すために同じ素子符号が使用されている。この詳細な説明では、以下を含む種々の用語が使用されている。
【００１７】
アプライアンス：デジタル情報を獲得し、その情報を送信し、位置情報を獲得するための最小容量を備えた電子デバイス、システム、ネットワーク、およびそれに類似したもの。これらの電子デバイスは、プログラム命令を実行するための処理機能、および短期および長期データ記憶用のメモリ容量を含んでいることが多い。
【００１８】
位置識別属性の関連付け：デジタル情報に位置識別属性を付ける方法。
【００１９】
デジタル情報：デジタル情報はデジタルフォーマットで表された情報である。デジタル的に表されることのできる情報の例には、テキスト、データ、ソフトウェア、音楽、ビデオ、グラフィックス等が含まれる。
【００２０】
位置識別属性の実施：デジタル情報の関連した位置識別属性によってそのデジタル情報へのアクセスを行うか、あるいは拒否する方法。
【００２１】
ジオコード：通常座標系に関連した地球上の位置の特有の符号化。いくつかのジオコードは、ある場所がその緯度および経度によって何時識別されたかのような、ポイント位置を識別する。別のジオコードは、郵便番号のような領域を識別してもよい。
【００２２】
ジェオロック：デジタル情報と、位置識別属性により規定された地理的エリアとの間において実施された関連付け。
【００２３】
ジェオロックされた情報：位置識別属性と関連付けられており、位置識別属性により規定されたエリア内においてのみアクセス可能なデジタル情報。
【００２４】
位置：任意の地理的な場所。それは、正確な地点、エリアまたは領域の位置、最も近いエリア内に含まれている地点、または地球上の場所の組合せであることができるが、それに限定されない。位置はまた、地球の表面より高いか、または低いポジションを識別するための高さ（または高度）、あるいは時間的なディメンションでポジションを識別するための時間を含むことができる。
【００２５】
位置識別属性：位置の正確な符号化。情報がアクセスされた位置を正確に規定するためにその情報の属性が使用されることができるが、それに限定されない。位置識別属性は、ある地点、ある領域、関連付けられた地点を有する領域、回廊地帯（すなわち、中心線の両側に長さを有するその中心線）の符号化であってもよいし、あるいはある位置の任意の他の正確な空間的および時間的識別により行われてもよい。
【００２６】
位置分散：ある位置のジオコードがそれと隣接した位置とを正確に区別できない可能性のある最小分解能。たとえば、軍用方眼地点指示方式が精度の２つのキャラクタと共に使用された場合、任意の位置の精度はわずか１０キロメートル以内である。
【００２７】
再生位置：デジタル情報の再生が許可されるであろう位置。
【００２８】

近接：その位置を含んでいるゾーンまたはエリア。

【００２９】

上記の定義は本発明の技術的範囲を制限するものではなく、それはむしろ本発明を説明するときに使用される用語を明確にするものである。定義された用語はまた、当業者には別の意味があることを認識すべきである。以下の詳細な説明において、これらおよびその他の用語が使用される。

【００３０】

図１を参照とすると、位置識別属性によって決定されたデジタル情報へのアクセスを表す本発明の概略図が示されている。位置識別属性とは、情報がアクセス可能な地理的エリアまたは領域を正確に決定するその情報の属性のことである。ＡおよびＢで示された２つの地理的エリアがマップ１０１上のアメリカ大陸内に示されている。情報１３０はデジタルフォーマットで表され、そのデジタル情報がアクセスされることのできる領域として地理的エリアＡを正確に規定する関連した位置識別属性１３１を有している。アプライアンス１１２がこの地理的領域Ａ内に位置している場合、デジタル情報１３０はそのアプライアンスによってアクセス可能となる。反対に、アプライアンス１２２がこの地理的領域Ｂ（または地理的領域Ａ以外の他のどこかの場所）内に位置している場合、デジタル情報１３０はアクセス不可能となるであろう。したがって、位置識別属性は、デジタル情報がアクセスされることのできる正確な地理的領域を決定するそのデジタル情報の属性を表している。位置識別属性を有するデジタル情報は“ジェオロックされている”と呼ばれ、位置識別属性を実施するシステムは関連付けられたデジタル情報を、位置識別属性により規定された地理的領域にジェオロックする。

【００３１】

図２には、位置識別属性１４０が情報の２つの項目、すなわち位置値１４２および近接値１４３を含むものとして示されている。位置値１４２は特定の場所の特有のポジションに対応している。任意の位置が特有に数値で識別される緯度および経度のような多くの異なった座標系が開発されている。本発明の目的のために、ある場所を特有に識別する任意の座標系が位置識別属性１４０の位置値１４２として使用されることができる。近接値１４３は、その位置を囲むゾーンまたはエリアの範囲に対応している。位置識別属性１４０は、近接値１４３がゼロ、ナル、空等、または位置識別属性により参照されたエリアが特有の地点であることを示すある別の値に設定されている場合、ある地点または正確な位置を含んでいてもよい。近接値１４３は、位置分散とは異なっていることを認識すべきである。近接値１４３はエリアまたは領域を表わすものであり、一方位置分散は、ジオコードが正確にそれと隣接した位置とを区別できない可能性のある最小分解能である。

【００３２】

図３は、位置値１４２をさらに詳細に示している。上述のように、座標系内の全ての各位置を特有に識別する１組の数が得られる多くの種々の座標系が一般的に使用されている。本発明において、位置値１４２は、１４２ａで示されているように特有の位置表示またはジオコードに関して規定される。それ故、通常の座標系を使用する緯度１４４および経度１４５がさらにジオコードを規定することができる。地球中心方式（Ｅａｒｔｈ Ｃｅｎｔｅｒｄ）のような既知の別のシステムにおいては、地球固定ガウス座標系、ユニバーサル・トランスバース・メルカトル（ＵＴＭ）、軍用方眼地点指示方式（ＭＧＲＳ）、ワールド・ジェオグラフィック・リファレンス・システム（ＧＥＯＲＥＦ）等もまた便利に使用されることができる。緯度１４４および経度１４５に加えて、位置値はさらに、１４２ｂで示されているように高度１４６を含むことが可能であり、この高度１４６は海水面より上方の位置の高さに対応している。その代りに、位置値はさらに、日付および、または時間範囲に関して規定されてもよい時間値１４７を含むことができる。これによって、位置識別属性の定義は情報に対する地理的および、または時間的アクセスの両者を考慮することが可能になる。

【００３３】

位置識別属性の位置値１４２を含む地理的領域またはエリアはいずれも位置識別属性１４

０に対する近接値１４３として機能することができる。近接値１４３は、２つの隣接した経度線（水平線のエッジを示す）と２つの隣接した緯度線（垂直線のエッジ）とにより規定された方形領域を含んでいてもよい。その代りに、近接値１４３は、その位置の周囲の半径を規定する単一の数により表された円形領域を含んでいてもよい。円形領域はさらに、その位置を中心とした楕円形エリアか、あるいは必ずしも質量中心としてではないがその位置を含んでいる円形または楕円形エリアのいずれかとして規定されることができる。別の形態では、近接値１４３は不規則的な閉じた多角形または回廊を含んでいてもよい。さらに別の形態においては、近接値１４３はブラジルの国のような既知の地理的領域に対応していてもよい。近接値１４３を規定することのできる既知の地理的領域の別のタイプには、郵便番号、州、郡、合併された市等が含まれる。

【００３４】

本発明によると、デジタル情報が保存されるか、記憶されるか、あるいはコピーされた場合には常に、デジタル情報の後続するアクセスが位置識別属性１４０により規定された地理的エリアに制限されるように、位置識別属性１４０がそのデジタル情報と関連付けられる。図４は、デジタル情報のアクセスまたは再生が可能にされるであろう領域を正確に規定する位置識別属性１４０とそのデジタル情報を関連付ける一般的な方法を示している。この方法は、コンピュータファイルが保存される場合のそのファイルに対する読出し専用属性のようなファイル属性の設定に類似していることを認識すべきである。この方法は、パーソナルコンピュータ、サーバ、パーソナル・デジタル・アシスタント（ＰＤＡ）、ラップトップ、ワークステーション、ネットワークおよびそれに類似したもののような別のパーティへの通信または配信のためにデジタル情報を生成し、操作し、処理するのに十分なデータ処理能力およびメモリを有するシステムまたはデバイスによって行われる。システムまたはデバイス上で動作するソフトウェアまたは埋込み型ファームウェア命令はこの方法が行われるようにする。

【００３５】

とくに、この方法は、位置識別属性と共にデジタル情報を保存または記憶するコマンドによりステップ２００からスタートする。ステップ２０２において、デジタル情報に対する位置値１４２は、後で使用するために検索され、記憶される。位置値１４２は、必ずしも、この方法がそのアプライアンスに呼出される地理的位置とは限らず、むしろデジタル情報に対するアクセスが許されることとなるアプライアンスに対する位置識別属性（上述した）に対応する。ステップ２０４において、アプライアンスの位置識別属性の近接値１４３が後で使用するために検索されて記憶される。以下、位置および近接値１４２、１４３を生成する種々の方法をさらに詳細に説明する。このような方法に加えて、位置および近接値１４２、１４３はまたメモリ中に予め記憶され、そこから検索されてもよいし、あるいはエンドユーザがその情報を提供するように問合せてもよい。ステップ２０６において、検索された位置および近接値１４２、１４３は、位置識別属性１４０を生成するために使用される。その後、ステップ２１０において、デジタル情報２１６は、ジェオロックされたデジタル情報２１８を提供するように位置識別属性１４０と関連付けられる。

【００３６】

再生アプライアンスが有効な位置識別属性を確認しない限り、そのアプライアンスより行われる読出しまたはコピー動作によってジェオロックされた情報にアクセスしようとする試みは、拒否されるであろう。これは、デジタル情報の関連付けられた位置識別属性を、再生アプライアンスの位置に対して評価して一致するか否かを決定することにより行われる。図５は、デジタル情報へのアクセスを位置識別属性により実施するための一般的な方法を示している。論理的には、この方法は、オペレーティングシステムが現在ファイル上で読出し専用属性を実施している方式、すなわちユーザが読出しのためにそのファイルにアクセスすることを許すが、書込みのためのアクセスを拒否する方式に類似している。この方法は、パーソナルコンピュータ、サーバ、ルータ、パーソナル・デジタル・アシスタント（ＰＤＡ）、ワークステーション、ネットワーク、ラップトップ等の別のパーティにより通信され、あるいは配信されたデジタル情報の受信を可能にするのに十分なデータ処

理能力またはメモリを有するシステムまたはデバイスによって行われる。システムまたはデバイス上で動作するソフトウェアまたは埋込み型ファームウェア命令はこの方法が行われるようにする。

【００３７】

とくに、この方法は、デジタル情報にアクセスするコマンドによりステップ２２０からスタートする。ステップ２２２において、ジェオロックされたデジタル情報２１８は、関連付けられた位置識別属性１４０を読出して記憶するためにアクセスされる。デジタル情報それ自身ではなく、ジェオロックされた情報の位置識別部分だけがアクセスされることを認識すべきである。ジェオロックされた情報の位置識別属性１４０はこの方法においてさらに使用されるために記憶される。ステップ２２４において、この方法は、デジタル情報にアクセスしたアプライアンスの位置を決定する。以下に説明するように、アプライアンス位置１６０を決定するための種々の可能な方法が存在する。アプライアンス位置１６０はこの方法においてさらに使用されるために記憶される。ステップ２２６において、この方法は、アプライアンスの位置が位置識別属性１４０により規定された領域と一致するか否かを決定する。アプライアンス位置１６０が位置識別属性１４０と一致した場合、ステップ２２８においてジェオロックされたデジタル情報２１８へのアクセスが可能にされる。反対に、アプライアンス位置１６０が位置識別属性１４０と一致しない場合、ステップ２３０においてアクセスは拒否される。

【００３８】

図６のＡ乃至Ｄは、ジェオロックされたデジタル情報へのアクセスを試みているアプライアンスの再生位置を決定するための複数の例示的な方法を示している。これらの方法は、図４に関して上述したように、デジタル情報による位置識別属性を実施する手順の一部分としてシステムにより行われる。アプライアンスの再生位置を決定する別の方法もまた便利に使用されることが可能であることを認識すべきである。

【００３９】

図６のＡは、ジェオロックされたデジタル情報を受信することとなるアプライアンスに対する街路アドレスからジオコードが解かれるアドレスデコード方法２４０を示している。ステップ２４２において、アプライアンスに対するアドレスが検索される。アドレス情報は、アドレスが獲得されたそのアプライアンスとの前の通信に基づいてメモリから再現されることができる。その代わりに、アプライアンスは情報トランザクションの最初の部分としてアドレス情報を与えるように考慮されてもよい。アドレス情報は一度検索されると、ステップ２４４において特定のジオコードを導くために復号される。このステップは、Ｍａｐｉｎｆｏ社（Ｔｒｏｙ，Ｎｅｗ　Ｙｏｒｋ）製のＭａｐＭａｒｋｅｒ　ＯＣＸコンポーネント　バージョン４．２のような、アドレスから座標特定ジオコードを生成することのできる市販のソフトウェアプログラムを使用してもよい。位置識別属性に関して時間要素を含むことが所望された場合、ステップ２４６において、アプライアンスシステムクロックから時間を読出す等によりそのアプライアンスから現在の時間が検索される。このステップ２４６は随意であり、多くのアプリケーションにおいて、時間要素は必要とされないことを認識すべきである。最後に、ステップ２４８において、ジオコードおよび時間は、位置識別属性１４０に対する位置値１４２として使用可能なフォーマットに変換される。

【００４０】

図６のＢは、アプライアンス上に記憶されたライセンスから位置値が導かれるアプライアンスライセンス方法２５０を示している。ライセンスパックは多くのシステムのよく知られている特徴であり、一般にアプライアンスプログラムへのアクセスの妥当性を検査するために使用されている。ライセンスパックは、ユーザ／免許された者に関する情報を含むデジタルファイルである。それらは解読不可能ではないが、ユーザの妥当性を検査する信頼性の高い方法のものとなるように編成され、暗号化されている。本発明のこの実施形態において、ライセンスパックは、アプライアンスの位置を識別する座標特定ジオコードを含んでいる。ステップ２５２において、アプライアンス上に記憶されたライセンスパック

がアクセスされ検索される。その後、ステップ２５４においてジオコードがそのライセンスから復元される。位置識別属性に関して時間要素を含むことが所望された場合、ステップ２５６において、アプライアンスシステムクロックから時間を読出す等によりそのアプライアンスから現在の時間が検索される。このステップ２５６は随意であり、多くのアプリケーションにおいて、時間要素は必要とされないことを認識すべきである。最後に、ステップ２５８において、ジオコードおよび時間は、位置識別属性１４０に対する位置値１４２として使用可能なフォーマットに変換される。

【００４１】

図６のＣは、アプライアンス内に埋込まれたＧＰＳ受信機から位置値が復元されるＧＰＳデータ復元方法２６０を示している。技術的に知られているように、グローバル・ポジショニング・システム（ＧＰＳ）は、米国防省により開発されて運用されている衛星ベースの無線航法システムである。ＧＰＳにより、地上、海上および航空機上のユーザは一日２４時間にわたって、全天候の下に、世界中のどこででも彼等の３次元位置、速度および時間を判断して決定することが可能となる。このＧＰＳシステムは民間ユーザに１００ｍ未満の正確度を提供し、一方軍事ユーザははるかに高い正確度を有している。ＧＰＳ位置情報は、Ｗｏｒｌｄ　Ｇｅｏｄｅｔｉｃ　Ｓｙｓｔｅｍ１９８４（ＷＧＳ８４）と呼ばれる座標系に基づいており、緯度および経度座標系に類似している。ＧＰＳ受信機の商業的可用性は、益々一般的になっており、この実施形態では、アプライアンスは組込み型ＧＰＳ受信機を含んでいることが予想される。たとえば、ＧＰＳ受信機は、Ｒｏｃｋｗｅｌｌ社製のＮａｖＣａｒｄまたはＴｒｉｍｂｌｅ　Ｎａｖｉｇａｔｉｏｎ社製のＧＰＳｃａｒｄのようなＰＣＭＣＩＡカードとして利用可能であり、Ｎｏｖａｌｅｌ社は汎用ＩＢＭ　ＰＣ用のＧＰＳ受信機を製造している。ステップ２６２において、アプライアンス内に組込まれたＧＰＳ受信機がアクセスされる。ステップ２６４において、組込まれたＧＰＳ受信機からジオコードが復元され、再生される。随意に、時間値もまたＧＰＳ受信機から復元されてもよい。最後に、ステップ２６６において、ジオコードおよびオプションの時間値は、位置識別属性１４０に対する位置値１４２として使用可能なフォーマットに変換される。

【００４２】

図６のＤはアプライアンスの位置を決定するための三角測量データ復元方法２７０を示している。技術的に知られているように、三角測量は、正確な位置情報を提供するために衛星、広域携帯電話、航法システムおよびその他の無線信号オペレータによってよく使用される方法である。ロランーＣシステムは、複数の固定された位置のＲＦ送信機からのＲＦ信号を三角測量することによって位置情報を提供する商用として利用可能な航法システムの一例である。ステップ２７２において、システムはアプライアンスにより伝達されたＲＦ信号にアクセスすることによりそのアプライアンスの方向を決定する。ステップ２７４において、三角測量アルゴリズムを使用してＲＦ信号からジオコードが計算される。最後に、ステップ２７６において、ジオコードは、位置識別属性１４０に対する位置値１４２として使用可能なフォーマットに変換される。位置識別属性において時間要素が必要とされた場合、上述した同じ方法でアプライアンスシステムクロックから現在の時間が読出される。

【００４３】

本発明の１実施形態によると、デジタル情報はアプライアンスへの転送前に暗号化され、位置識別属性１４０は、デジタル情報を暗号化するために使用される位置識別属性ベースのキーを生成するために使用される。デジタル情報に追加される暗号の層は、位置識別属性１４０により規定されたアクセスに対する制限を実施する。図７は、デジタル情報を位置識別属性１４０と関連付ける暗号化方法を示している。この方法は、位置識別属性と共にデジタル情報を保存または記憶するコマンドによりステップ３００からスタートする。ステップ３０２において、デジタル情報に対する位置値１４２が検索され、後で使用されるために記憶される。ステップ３０４において、アプライアンスの位置識別属性の近接値１４３は検索され、後で使用されるために記憶される。ステップ３０６において、位置お

よび近接値１４２、１４３はエリアパラメータ１９０を生成するために使用され、このエリアパラメータは位置および近接値により規定された地理的領域の形状を規定するが、しかしそれは位置の識別はしない。このエリアパラメータ１９０は、近接値１４３に対応していてもよい。ステップ３０８において、暗号位置識別属性キー１７０を生成するために位置および近接値１４２、１４３が使用される。その後、ステップ３１０において、クリアテキスト形式のデジタル情報３１２は、暗号化されたジェオロックされたデジタル情報３１４を暗号テキスト形式で供給するために暗号アルゴリズムにより位置識別属性キー１７０と決定論的に組合せられる。この方法では、位置識別属性がデジタル情報と暗号法に基づいて統合されるように、クリアテキストが位置識別属性キー１７０に基づいて暗号化される。ステップ３１４において、エリアパラメータ１９０はまたクリアテキスト形式でジェオロックされたデジタル情報に取付けられる。エリアパラメータだけでは位置識別属性キーを生成するのに不十分である限り、しかし、位置識別属性キーを生成するためにアプライアンスの位置と組合せられる場合にのみ、エリアパラメータ１９０を生成する別の方法が使用されてもよいことを認識すべきである。

【００４４】

再生アプライアンスにより行われる読出しまたはコピー動作により、暗号化されたジェオロックされたデジタル情報３１４にアクセスしようとする試みは、そのアプライアンスが位置識別属性を実施しない限り、拒否される。図８は、暗号化位置識別属性によりジェオロックされたデジタル情報へのアクセスを実施する方法を示している。この方法は、デジタル情報にアクセスするためのコマンドによりステップ３２０からスタートする。ステップ３２２において、暗号化されたジェオロックされたデジタル情報３１４は、エリアパラメータ１９０を復元するためにアクセスされる。この時点でエリアパラメータ１９０だけがアクセスされ、暗号化されたジェオロックされた情報はアクセスされないことを認識すべきである。ステップ３２４において、この方法は、上述した方法の１つを使用する等によって、デジタル情報にアクセスしたアプライアンスの位置を決定する。この方法で将来使用するために、アプライアンス位置１６０が記憶される。方法はステップ３２８に進み、このステップにおいて、暗号化位置識別属性キー１７０を生成するためにアプライアンス位置１６０がエリアパラメータ１９０と組合せられる。ステップ３２８において生成された暗号化位置識別属性キー１７０は、アプライアンス位置１６０が位置識別属性により規定された領域の範囲内に位置している場合にのみ、前にステップ３０８において生成された暗号化位置識別属性キー（上記を参照）と一致することを認識すべきである。その後、ステップ３３０において暗号化位置識別属性キー１７０は、ジェオロックされたデジタル情報３１４を解読してクリアテキストデジタル情報３１２を生成するために暗号アルゴリズムにおいて使用される。この方法は、どの特定のタイプの暗号アルゴリズムにも依存しておらず、秘密キー暗号化および公開キー暗号化を含む既知のどの暗号化方法による使用にでも適応可能であることが認められる。

【００４５】

本発明の別の実施形態において、アプライアンスのアプリケーションまたはオペレーティングシステムによるデジタル情報への後続的なアクセスが、位置識別属性１４０により特定された地理的エリアに制限されるように、この位置識別属性１４０は、そのアプリケーションまたはオペレーティングシステムによりデジタル情報を含むファイルと関連付けられる。主にパーティ間でのデジタル情報の通信に関して説明された図４の実施形態（上述の）とは異なり、この実施形態は個々のアプライアンスまたはアプライアンスのネットワーク上で実行するアプリケーションプログラムまたはオペレーティングシステムによるデータファイルの管理に最も適切である。とくに、この方法は、ファイルへのアクセスを決定するためにワード処理プログラム、ｅメールクライアントまたはデータベースマネジャのような、アプリケーションプログラムにより使用されるファイルと共に（たとえば、ファイルヘッダ中に）位置識別属性を含むことに関する。オペレーティングシステムは、保存、記憶、コピー、削除および読出しコマンドを含む基本的なシステムファイル動作を制御するドライバ中に本発明の方法を組み込むことが可能であることを認識すべきである。

これは、読出し／書込み属性のようなファイル属性がＵＮＩＸ、ＷｉｎｄｏｗｓおよびＶＡＸ／ＤＣＬオペレーティングシステムで処理される方法に類似している。

【００４６】

図９は、アプリケーションまたはオペレーティングシステムによるデジタル情報ファイルのアクセスが可能にされることとなる領域を正確に規定する位置識別属性１４０とデジタル情報を関連付けるファイル方法を示している。この方法は、位置識別属性と共にデジタル情報を含むファイルを保存または記憶するコマンドによるステップ４００からスタートする。このコマンドは、アプリケーションまたはオペレーティングシステムの通常の動作の一部分として行われてもよい。ステップ４０２において、デジタル情報に対する位置値１４２が検索され、後で使用されるために記憶される。ステップ４０４において、アプライアンスの位置識別属性の近接値１４３が検索され、後で使用されるために記憶される。上述したように、位置および近接値１４２、１４３を生成する種々の方法が使用可能である。ステップ４０６において、検索された位置および近接値１４２、１４３は、位置識別属性１４０を生成するために使用される。その後、ステップ４０８において、デジタル情報４１６は、ジェオロックされたデジタル情報４１８を提供するためにこの位置識別属性１４０と統合される。デジタル情報４１６を関連付けられた位置識別属性１４０と統合する多数の方法が存在する。ファイルとして記憶されるデジタル情報４１６に対して、位置識別属性はフォーマット化され、ヘッダ中のように、デジタル情報ファイルのフロントに添付されることができる。その代りに、位置識別属性１４０は関連付けられたディレクトリファイル中に保存されることができる。いずれの場合にも、デジタル情報ファイルへのアクセスを試みたアプリケーションまたはオペレーティングシステムは、その位置識別属性１４０がジェオロックされたデジタル情報へのアクセスを可能にするか否かを決定することによって位置識別属性を実施するであろう。

【００４７】

アプライアンス上で実行するアプリケーションまたはオペレーティングシステムにより行われる読出しまたはコピー動作によってジェオロックされた情報にアクセスしようとする試みは、そのアプライアンスが位置識別属性に従わない限り拒否されるであろう。図１０は、ジェオロックされたデジタル情報へのアクセスを位置識別属性によって実施するファイル方法を示している。この方法は、ジェオロックされたデジタル情報にアクセスするコマンドによりステップ４２０からスタートする。ステップ４２２において、ジェオロックされたデジタル情報２１８は関連付けられた位置識別属性１４０を復元するためにアクセスされる。ジェオロックされた情報の位置識別部分だけがアクセスされ、デジタル情報自身はアクセスされないことを認識すべきである。ステップ４２４において、この方法はデジタル情報にアクセスしたアプライアンスの位置を決定する。上述したように、アプライアンス位置１６０を決定する種々の可能な方法が存在する。この方法において将来使用するためにアプライアンス位置１６０は記憶される。ステップ４２６において、この方法は、そのアプライアンスの位置が位置識別属性１４０により規定された領域と一致するか否かを決定する。アプライアンス位置１６０が位置識別属性１４０と一致した場合、ステップ４２８においてアプリケーションまたはオペレーティングシステムはジェオロックされたデジタル情報２１８にアクセスすることができる。反対に、アプライアンス位置１６０が位置識別属性１４０と一致しない場合、ステップ４３０においてアクセスは拒否される。ジェオロックされたデジタル情報へのアクセスはアプリケーションまたはオペレーティングシステムによってのみ行われることが可能であるため、そのアプリケーションまたはオペレーティングシステムは、ジェオロックされたデジタル情報へのアクセスを頑強に実施することができるであろう。

【００４８】

本発明のさらに別の実施形態において、位置識別属性１４０とデジタル情報を関連付ける方法は、アプライアンスに対するハードウェアコントローラにおいて行われることができる。アプライアンスに対するあらゆるハードウェアデバイス（たとえば、ハードディスク、ＤＶＤ／ＣＤ－ＲＯＭ、フロッピーディスク、ビデオディスプレイ等）は、ソフトウェ

アオペレーティングシステムからの特定のコマンドに応答して限定された機能セットをそのデバイスで行う対応したハードウェアコントローラを有している。上記の実施形態におけるように、デジタル情報は対応した位置識別属性と関連されて保存される。デバイスレベルのコマンドによりデジタル情報を読出そうとする試みは、再生アプライアンスの位置およびそのデバイスに記憶された位置識別属性に関してそのデバイスハードウェアコントローラによってのみ実行されるであろう。

【００４９】

とくに、ハードウェアコントローラは、図４に関して上述した一般的な方法のステップ２０２乃至２１０ならびに図５に関して上述した一般的な方法のステップ２２２乃至２３０を含む上述の方法のいくつかまたは全ての特徴を実行するように構成されることができる。たとえば、パーソナルコンピュータ用のハードディスクコントローラは、ハードディスク中に記憶されたあらゆるデジタル情報ファイルがそれと共に、あるいはファイルディレクトリの一部分として記憶された位置識別属性を有するように、上述の方法を行うように符号化されてもよい。デバイスハードウェアコントローラはさらに、デバイスハードウェアコントローラに位置および時間情報を提供することのできる統合されたＧＰＳ受信機を含んでいてもよい。

上記のように、記憶されたファイルにアクセスしようとする試みは、アプライアンス位置がその位置識別属性と一致しない限り、ハードウェアコントローラにより阻止されるであろう。同様に、ビデオコントローラは、アプライアンス位置がその位置識別属性と一致しない限り、ファイルの表示を阻止するように符号化されてもよい。

【００５０】

デジタル情報へのアクセスを制御するために位置識別属性が使用されることのできる種々のアプリケーションおよびデータフォーマットが存在している。ユーザはジェオロックされたデジタル情報を、電話線、光ファイバ、ケーブルテレビジョン、衛星放送、無線またはその他のメディアを含む任意の通常の方法を使用して電子形態で受信することができる。ユーザはまた注文生成されたジェオロックされたデジタル情報を、たとえばＣＤ－ＲＯＭ、ディスケット、ビデオカセットまたはテープ等の磁気または別の符号化されたメディアの形態で店またはベンダーから物理的に受取ることができる。同様に、ジェオロックされたデジタル情報は、インターネットのような広域ネットワーク、イントラネットのようなローカルネットワーク、ｅメールへの接続機構としての、あるいはデジタル広域形態電話または別の無線デバイスによるパーソナルおよびサーバコンピュータ間のダイヤルアップアクセスを含むネットワークによって伝送されることができる。ジェオロックされたデジタル情報はディスケット、ＣＤ－ＲＯＭ、テープ、固定または取外し可能なハードディスク、ＤＶＤ／ＣＤ－ＲＯＭ、フラッシュメモリ／ディスク、ＥＥＰＲＯＭ等に記憶されることができる。これに関して保護されることのできるデジタル情報のタイプは、いくつか名をあげると、音楽ファイル（たとえば、ＭＰ３）、ソフトウェア、著作物、商業取引ファイル、テキストファイル、ビデオ／グラフィックス、ページングメッセージ、広域携帯電話の会話および交渉、ならびにデジタルフィルムを含むことができる。

【００５１】

本発明の例示的なアプリケーションにおいて、位置識別属性はデジタルフィルムの著作権侵害および無許可使用ならびにコピーの問題を克服するために使用されてもよい。顧客は、ビデオレンタル店でフィルムを借りるか、あるいは購入する場合と類似した方法でデジタルビデオメディア（たとえば、ＤＶＤ）を借りるか、あるいは購入する。位置識別属性は、デジタルビデオメディアの購入時に使用される。とくに、顧客の家のアドレスに対応した位置識別属性は、デジタルビデオメディアの再度書込み可能な部分の上に物理的に記憶される。顧客の家庭にあるＤＶＤプレーヤは、デジタルビデオメディアの再生を特定の地理的領域および時間期間に制限するために位置識別属性を実施するようにコード化される。このメディアは、それがコピーされるか、紛失するか、あるいは盗まれた場合でさえ、その再生領域および時間期間内だけは見られることができ、したがってデジタルメディアの無許可使用に関連した問題に対する頑強な解決方法として機能する。

【００５２】
別の例示的なアプリケーションにおいて、顧客はデジタルフィルムまたはオーディオをベンダーのカタログから注文する。このカタログはハードコピーまたはインターネットベースのものであってよく、その注文は郵便投函、電話、ファクシミリ送信またはインターネットベースの取引によって行われることができる。何れの発注方法でも、顧客の注文は再生位置を示している。この注文がベンダーによって調達されたときに、その顧客に関連した位置識別属性が決定され、暗号キーを生成するために使用され、後にこの暗号キーはそのメディアに対するデジタル情報ファイルを暗号化するために使用される。その後、購入されたメディアはその注文に対してカストマ暗号化され、ＤＶＤまたはＣＤ－ＲＯＭのようなフォーマットにコピーされ、ビューアと共にパッケージ化され、このビューアもまた位置識別属性に対してカストマイズされている。購入されたメディアの内容全体がコピーされた場合でさえ、その位置識別属性に対してカストマ化されているビューアおよびメディアが許容領域外での視聴を阻止する。この例示的なアプリケーションでは、位置識別属性ならびにカストマイズされた暗号およびビューアの使用により、デジタルメディアの著作権侵害および無許可使用ならびにコピーの問題に対して抵抗力の強い解決方法が提供される。

【００５３】
本発明の別の例示的なアプリケーションにおいて、位置識別属性は、公衆ネットワークによって情報を“有線放送（ｎａｒｒｏｗｃａｓｔ）”するために使用される。有線放送とは、限られた視聴者に対する情報の伝送（情報が大衆に伝送される放送とは対照的に）のことである。たとえば、局地的天候、交通情報、映画上映スケジュール、店舗情報等の多くのタイプの情報は、ある位置関係の範囲内でのみ使用可能である。このような位置依存性情報を使用するアプリケーションは、位置ベースアプリケーションと呼ばれることができる。位置識別属性は、たとえば、天候に対するローカル地域、販売に対する店舗の位置および広告情報等の、それが関連する位置で識別されるネットワークによって情報を送信するために放送タイプのプロトコルを使用する方法を提供する。クライアントのアプライアンスの位置を使用することにより、そのクライアントのアプリケーションは情報に付与された位置識別子を使用して、それらの現在の位置に基づいて情報を選択的にスクリーンすることができる。それはまた、地理的に制限された有線放送アプリケーションに対して、機密保護されて安全な秘密通信を維持するために特有の位置ベースの共用暗号キーを設定する方法を提供することができる。

【００５４】
本発明の別の例示的なアプリケーションにおいて、位置識別属性は、無線ネットワーク連結性に対する機密性およびセキュリティを強化するために使用される。無線ネットワーキングは、無線ポータブルまたはワークステーションがネットワークに接続することを可能にする“ブルートゥース”テクノロジーのようなネットワーキング装置およびプロトコルの出現と共に成年に達した。“ブルートゥース”は移動デバイス（たとえば、ラップトップ、ＰＤＡ、広域携帯電話等）とポイント・ツー・ポイントおよびマルチポイントアプリケーションをサポートするデスクトップデバイスとの間におけるデジタル音声およびデータの短距離送信用の公然の標準規格である。ネットワークによって通信しているあらゆる無線アプライアンスは、特有の位置を有するため、位置識別属性は、公衆ネットワークによって接続した無線デバイスに対する安全な機密通信を維持するために使用されることのできる特有の共用暗号キーを設定するために使用可能である。

【００５５】
本発明のさらに別の例示的なアプリケーションにおいて、位置識別属性は、ウェブアプリケーションのユーザに対する機密性およびセキュリティを強化するために使用される。インターネット“クッキー”は、ウェブアプリケーションが別々のウェブページ間の状態を維持することを可能にする方法を提供し、サーバがユーザのコンピュータ上において名前／値対を設定して記憶することを可能にすることにより広く行われている。サーバは、設定されてクライアントおよびサーバにより共有される特有の状態識別子を含むユーザコン

ピュータにクッキーを配信する。しかしながら、サーバがユーザのコンピュータ上において情報を設定して記憶することが可能になることで、機密性およびセキュリティ問題が生じてきた。本発明は、サーバと共有されると共にウェブベースアプリケーションに対する状態を維持するために使用されることのできる特有の状態識別子をクライアントアプリケーションが生成することを可能にすることにより機密性およびセキュリティを強化する新しい方法を提供する。

【００５６】

上述した実施形態および例示的なアプリケーションのそれぞれにおいて、ジェオロックされたデジタル情報にアクセスするアプリケーションプログラムとこれらのアプリケーションが動作する周辺およびネットワーク環境との間には少なくとも４つの論理的な境界が存在する。これらの境界には、（１）データ獲得／アプライアンスの境界、（２）記憶／アプライアンスの境界、（３）ユーザインターフェース／アプライアンスの境界、および（４）アプライアンス／位置の獲得の境界が含まれる。データ獲得／アプライアンスの境界とは、たとえば、位置識別属性が満足されない限り別のソースからデジタル情報を獲得できないアプライアンス等のアプライアンスがデジタル情報を獲得した点で位置識別属性を実施することである。記憶／アプライアンスの境界とは、たとえば、位置識別属性が満足されない限り、アプライアンスは記憶されたファイルをメモリから呼出すことができない等の、アプライアンスがデジタル情報を記憶した時点で位置識別属性を実施することである。ユーザインターフェース／アプライアンスの境界とは、たとえば、位置識別属性が満足されない限り、ユーザはアプライアンスのモニタ上でデジタル情報を見ることができない等の、ユーザに情報を与えた時点で位置識別属性を実施することである。アプライアンス／位置の獲得の境界とは、たとえば、組込み型ＧＰＳ受信機を使用してそのアプライアンス位置が獲得されない限り、ユーザが如何なる方法でもそのデジタル情報を見たり、記憶したり、検索したりする、あるいはそうでなければ使用することができない等の、アプライアンス位置の妥当性を検査することによってジェオロックされたデータへのアクセスを制限することである。本発明の任意の特定の実施形態により提供される相対的なセキュリティは、アクセス制御が実施される境界に関連していることを認識すべきである。

【００５７】

以上、デジタル情報へのアクセスを制御するために位置識別属性を使用するシステムおよび方法の好ましい実施形態を説明してきたが、当業者には、本発明の利点が達成されていることが明らかであろう。本発明の技術的範囲内において種々の修正、適応および別の実施形態が可能であることもまた認識しなければならない。

【図面の簡単な説明】

【図１】

本発明の１実施形態にしたがって位置識別属性により決定されたデジタル情報へのアクセスを示す概略図。

【図２】

位置識別属性の構成要素を示すブロック図。

【図３】

位置識別属性の位置値の構成要素を示すブロック図。

【図４】

位置識別属性をデジタル情報と関連付けるための方法を示すフローチャート。

【図５】

ジェオロックされたデジタル情報へのアクセスを、位置識別属性を使用して実施するための方法を示すフローチャート。

【図６】

アプライアンスに対する位置識別属性を決定するための別の方法を示すフローチャート。

【図７】

位置識別属性をデジタル情報と関連付けるための暗号化方法を示すフローチャート。

【図８】

ジェオロックされたデジタル情報へのアクセスを、位置識別属性を使用して実施するための暗号化方法を示すフローチャート。

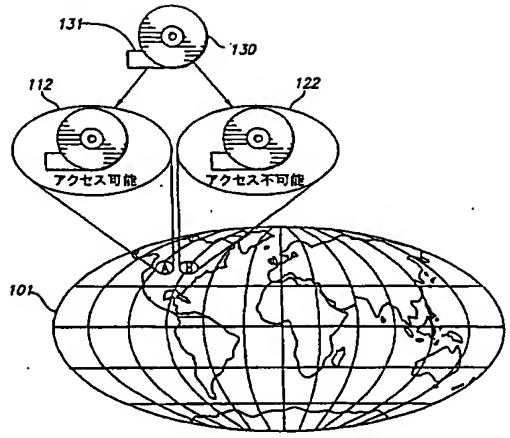
【図９】

位置識別属性をデジタル情報と関連付けるためのファイル方法を示すフローチャート。

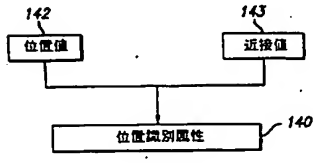
【図１０】

ジェオロックされたデジタル情報へのアクセスを、位置識別属性を使用して実施するためのファイル方法を示すフローチャート。

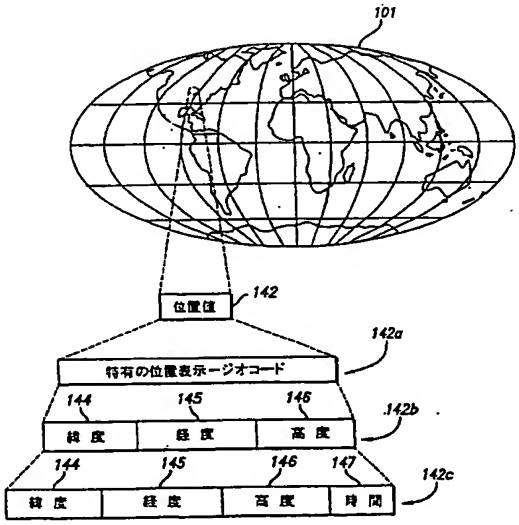
【図１】



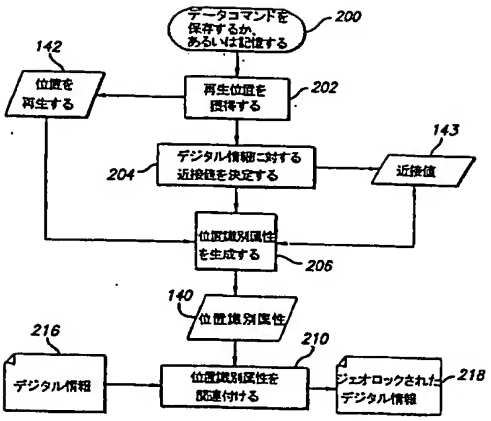
【図２】



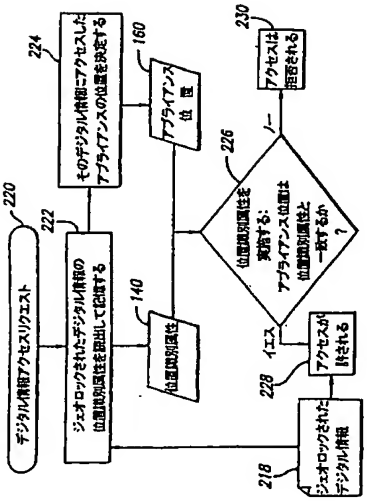
【図３】



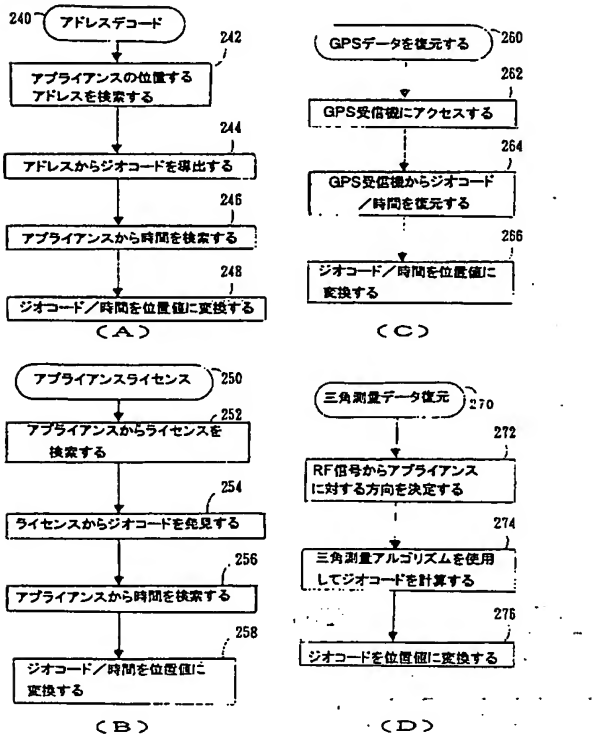
【図４】


データコマンドを保存するか、あるいは記憶する
200
142
位置を再生する
再生位置を獲得する
202
143
204
デジタル情報に対する近接値を決定する
近接値
位置識別属性を生成する
206
140
位置識別属性
216
デジタル情報
210
位置識別属性を関連付ける
ジオロックされたデジタル情報
218

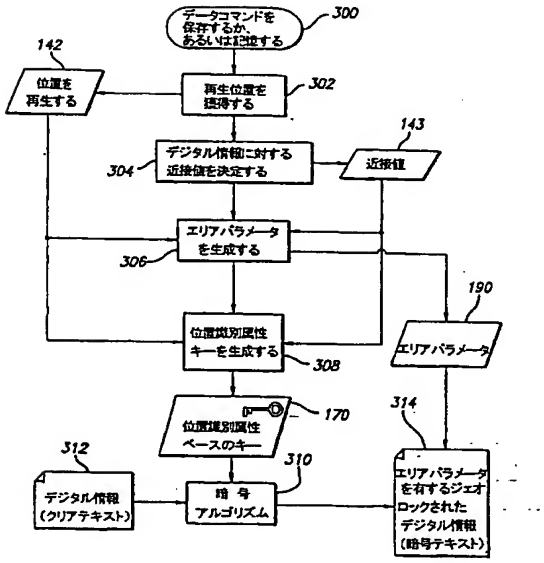
【図５】


224
そのデジタル情報にアクセスしたアプライアンスの位置を決定する
160
アプライアンス位置
230
アクセスは拒否される
ノー
226
位置識別属性を実行する：アプライアンス位置は位置識別属性と一致するか？
220
デジタル情報アクセスリクエスト
222
ジオロックされたデジタル情報の位置識別属性を抽出して記憶する
140
位置識別属性
イエス
228
アクセスが許される
218
ジオロックされたデジタル情報

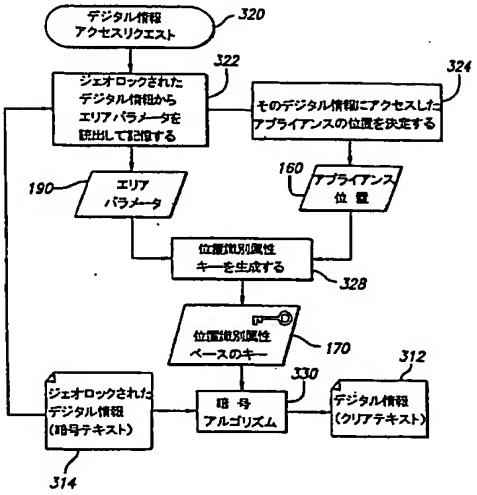
【図６】


240
アドレスデコード
242
アプライアンスの位置するアドレスを検索する
244
アドレスからジオコードを導出する
246
アプライアンスから時間を検索する
248
ジオコード／時間を位置値に変換する
（A）
アプライアンスライセンス
250
252
アプライアンスからライセンスを検索する
254
ライセンスからジオコードを発見する
256
アプライアンスから時間を検索する
258
ジオコード／時間を位置値に変換する
（B）
GPSデータを復元する
260
262
GPS受信機にアクセスする
264
GPS受信機からジオコード／時間を復元する
266
ジオコード／時間を位置値に変換する
（C）
三角測量データ復元
270
272
RF信号からアプライアンスに対する方向を決定する
274
三角測量アルゴリズムを使用してジオコードを計算する
276
ジオコードを位置値に変換する
（D）

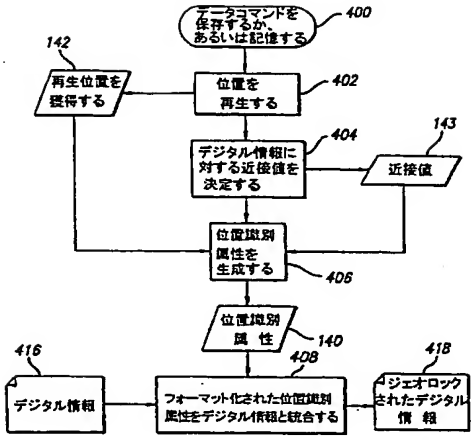
【図７】


データコマンドを保存するか、あるいは記憶する
300
142
位置を再生する
再生位置を獲得する
302
143
304
デジタル情報に対する近接値を決定する
近接値
エリアパラメータを生成する
306
190
位置識別属性キーを生成する
308
エリアパラメータ
170
位置識別属性ベースのキー
314
312
デジタル情報（クリアテキスト）
暗号アルゴリズム
310
エリアパラメータを有するジオロックされたデジタル情報（暗号テキスト）

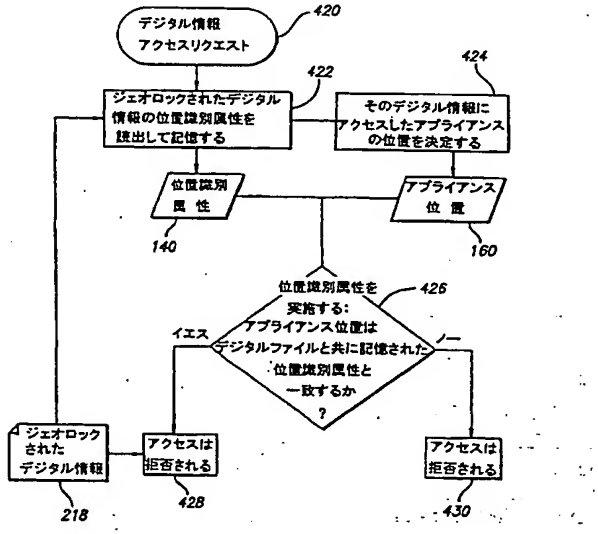
【図８】


デジタル情報
アクセスリクエスト
320
ジェオロックされた
デジタル情報から
エリアパラメータを
読出して記憶する
322
そのデジタル情報にアクセスした
アプライアンスの位置を決定する
324
190
エリア
パラメータ
160
アプライアンス
位置
位置識別属性
キーを生成する
328
位置識別属性
ベースのキー
170
330
暗号
アルゴリズム
312
デジタル情報
(クリアテキスト)
ジェオロックされた
デジタル情報
(暗号テキスト)
314

【図９】


データコマンドを
保存するか、
あるいは記憶する
400
142
再生位置を
獲得する
位置を
再生する
402
デジタル情報に
対する近接値を
決定する
404
143
近接値
位置識別
属性を
生成する
406
位置識別
属性
140
416
408
418
デジタル情報
フォーマット化された位置識別
属性をデジタル情報と統合する
ジェオロック
されたデジタル
情報

【図１０】


デジタル情報
アクセスリクエスト
420
ジェオロックされたデジタル
情報の位置識別属性を
読出して記憶する
422
そのデジタル情報に
アクセスしたアプライアンス
の位置を決定する
424
位置識別
属性
140
アプライアンス
位置
160
位置識別属性を
実施する:
アプライアンス位置は
デジタルファイルと共に記憶された
位置識別属性と
一致するか
?
426
イエス
ノー
ジェオロック
された
デジタル情報
218
アクセスは
拒否される
428
アクセスは
拒否される
430

【国際公開パンフレット】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 May 2002 (10.05.2002)

PCT

(10) International Publication Number
WO 02/37246 A2

(51) International Patent Classification⁷: G06F 1/00

(21) International Application Number: PCT/US01/48076

(22) International Filing Date: 30 October 2001 (30.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/699,832 30 October 2000 (30.10.2000) US

(71) Applicants and
(72) Inventors: SEILER, Mark [US/US]; 3480 Blair Drive, Los Angeles, CA 90068 (US). GLICK, Barry, J. [US/US]; 2710 Cathedral Avenue NW, Washington, DC 20008 (US). KARPF, Ronald, S. [US/US]; 13425 Brandy Hall Lane, Gaithersburg, MD 20878 (US).

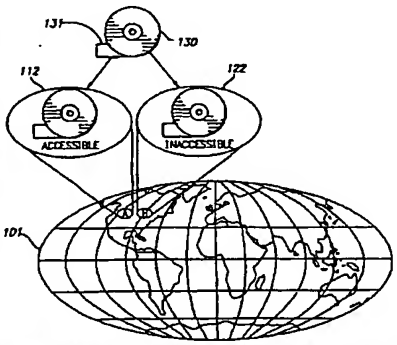
(74) Agents: BERLINER, Brian, M. et al.; O'Melveny & Myers LLP, 400 South Hope Street, Los Angeles, CA 90071-2899 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR USING LOCATION IDENTITY TO CONTROL ACCESS TO DIGITAL INFORMATION



(57) Abstract: A method and apparatus for controlling access to digital information utilizes a location identity attribute that defines a specific geographic location. The location identity attribute is associated with the digital information such that the digital information can be accessed only at the specific geographic location. The location identity attribute further includes a location value and a proximity value. The location value corresponds to a location of an intended recipient appliance of the digital information, and may be further defined in terms of latitude, longitude and altitude dimensions. The location identity attribute is enforced by allowing access to the digital information only at the specific geographic location. As a first part of this enforcement process, the location of an appliance through which access to the digital information is sought is identified. The appliance location is then compared to the specific geographic location defined by the location identity attribute, and access to the digital information is allowed only if the appliance location falls within the specific geographic location. There are many ways to identify the location of the appliance, including: (1) resolving the appliance location from a street address for the appliance; (2) retrieving the appliance location from a file stored within the appliance; (3) recovering the appliance location from a GPS receiver embedded in the appliance; and (4) recovering the appliance location by triangulating RF signals received by the appliance.

WO 02/37246 A2

WO 02/37246 A2

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR USING LOCATION IDENTITY TO CONTROL ACCESS TO DIGITAL INFORMATION

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the communication of digital information, and more particularly, to methods and systems for controlling interchange of digital information using a location integrity attribute associated with the digital information.

2. Description of Related Art

Rapid advances in computer, telecommunications and networking technology have enabled an avalanche of new opportunities and applications that were impossible just a few years ago. These advances are exemplified by the explosive growth in popularity of the Internet. As known in the art, the Internet is an interconnection of computer networks that enables computers of all kinds to communicate with each other and share information. Companies, individuals, government agencies, charitable organizations, and academic centers, of all sizes, regularly use the Internet to share information, deliver services, and exchange a wide range of content. The Internet functions as a distributed network of systems that is neither controlled nor managed by any one entity. Physical and logical pathways that facilitate the exchange of information connect these networks to each other.

In spite of the tremendous value that this information access has brought to society, there are also enormous costs associated with the uncontrolled flow of information. One of the most important considerations for a communication system is the control over information security and access. In many cases, a sender of information wants to ensure that the intended recipient can only access the information, and that any other unintended recipients of the information are denied access. This information security and access control is typically provided by an encryption system

that converts the information into a secret code for transmission over a public network. In an encryption system, the sender converts the original data, or "plaintext," into a coded equivalent called "ciphertext" using an encryption algorithm. The ciphertext may then be decoded (or decrypted) by the receiver and thereby turned back into plaintext. The encryption algorithm uses a key, which is a binary number that is typically from 40 to 128 bits in length. The greater the number of bits in the key, the more possible key combinations and the longer it would take to break the code. The data is encrypted, or "locked," by combining the bits in the key mathematically with the data bits. At the receiving end, the key is used to "unlock" the code and restore the original data.

There are two cryptographic methods in general use. The first method uses a secret key that is used by both the sender and receiver to encrypt and decrypt the plaintext information. A drawback of this method is that it is hard for the sender to deliver the secret key to the receiver without risking its compromise. The second method is known as public-key cryptography, which uses two keys known as a private and a public key. Each party has a private key that is kept secret and not shared, and a public key that is made publicly available. The public key is used to encrypt the plaintext information, and the private key is used to decrypt the ciphertext message. The private key may not be mathematically derived from the public key. The parties to a communication may exchange their public keys over an unsecured communication channel, such as the Internet, and thereafter use the public keys to encrypt their messages. The receivers then use the private key to decrypt the message.

Another important consideration for a communication system is the prevention of unauthorized copying of copyright-protected digital content. With conventional computing and communication systems, an unscrupulous individual can easily make and distribute an unlimited number of identical copies of a copyrighted work in digital form (e.g., music, literary works, photography, video, software, etc.). Moreover, commercially available file indexing services allow computer users to easily locate and access digital files on other user's computer systems, thereby greatly increasing the potential for widespread copyright piracy. One such service provided by Napster, Inc.,

of San Mateo, CA, provides a file sharing application that works in conjunction with Napster's Web site to locate music files in the popular MP3 format residing on other computers currently logged onto the Internet. A similar service known as Gnutella provides a file sharing system that allows users to search for software and documents on the GnutellaNet, a loose federation of users and organizations that make a wide variety of information available to the world at large. Gnutella differs from Napster, which is geared to music files and provides a centralized listing, whereas the GnutellaNet is a peer-to-peer network that contains all kinds of files. While these file sharing systems also have a legitimate purpose in enabling users to share non-copyright-protected files, they are also widely used to obtain copyright-protected files in violation of copyright laws. The illicit use of these file sharing systems represents a serious threat to copyright owners.

Active policing of the Internet is not a viable solution for copyright holders. Such policing efforts are logistically difficult given the widespread and anonymous nature of Internet copyright piracy. In addition, the popular sentiment that information content exchanged on the Internet should be free makes large scale policing efforts very unattractive from a public relations standpoint. To address this problem, various digital rights management (DRM) systems have emerged for protecting the copyrights of digital content that is distributed by focusing on preventative measures. For example, a proposed DRM system for the recording industry known as the Secure Digital Music Initiative (SDMI) sets forth a set of rules for securely distributing digital music over the Internet. SDMI provides guidelines for developing compliant DRM systems, including a container format that software and hardware players must support in order to play back the material. Announced in February 1999, the SDMI is backed by the Recording Industry Association of America (RIAA) and Sony, Warner, BMG, EMI and Universal, the top five music production companies.

Notwithstanding these efforts, DRM systems present at best an incomplete solution for a number of reasons. First, given the availability of pirated content on the Internet, it is far more convenient and inexpensive for a user to unlawfully download a

digital file over the Internet than to purchase a legitimate copy of the material via conventional channels of trade. While the unlawfully obtained material may have reduced quality in comparison to the legitimate copy, the convenience and negligible cost often make up for this drawback.

Second, most DRM technologies rely upon some form of encryption to protect the digital information. To be most effective, both parties to an encryption scheme must have a vested interest in maintaining the secrecy of the encrypted information. A legal purchaser of content has a right to view the content, but has no vested interest in ensuring that the secrecy afforded by encryption is maintained. For this reason, many DRM solutions utilize digital certificates or licenses that attempt to hide the decryption key from the user. In such systems, all copies of the content are encrypted in an identical manner, and the media player validates the user's right to display or play back the decrypted content. Since the encrypted content and decryption key are nevertheless accessible to the user albeit hidden, a sophisticated user may reverse engineer the DRM solution to strip away the encryption to thereby permit unimpeded copying and distribution of the decrypted content. Other less sophisticated ways of obtaining an unencrypted copy of the content are also available to unscrupulous users, such as videotaping each frame of a digital video data file as that content is legally displayed during playback.

Accordingly, it would be very desirable to provide a way to control the interchange of digital information that overcomes these and other drawbacks. More particularly, it would be desirable to provide an information interchange system and method that allows control over security and access to the information, and which prevents unauthorized copying of copyright-protected content.

SUMMARY OF THE INVENTION

A method and apparatus for controlling access to digital information in accordance with the present invention utilizes a location identity attribute that defines a specific geographic location. The location identity attribute is associated with the digital information such that the digital information can be accessed only at the specific

geographic location. The location identity attribute further includes a location value and a proximity value. The location value corresponds to a location of an intended recipient appliance of the digital information, and may be further defined in terms of latitude, longitude and altitude dimensions. The proximity value corresponds to a zone that encompasses the location. The location identity attribute may further include a temporal value such that the digital information can only be accessed at the specific geographic location and during a particular time period.

According to a general embodiment of the invention, access to the digital information is allowed only at the specific geographic location defined by the location identity attribute. As a first part of this enforcement process, the location of an appliance through which access to the digital information is sought is identified. There are many ways to identify the location of the appliance, including: (1) resolving the appliance location from a street address for the appliance; (2) retrieving the appliance location from a file stored within the appliance; (3) recovering the appliance location from a GPS receiver embedded in the appliance; and (4) recovering the appliance location by triangulating RF signals received by the appliance. . After the appliance location is identified, it is compared to the specific geographic location defined by the location identity attribute. Access to the digital information is allowed only if the appliance location falls within the specific geographic location.

In a more specific embodiment of the invention based on the foregoing general embodiment, the digital information is encrypted using an encryption key based at least in part on the location identity attribute. The encryption key may be further based on an area parameter that is determined from the location identity attribute and is included with the encrypted digital information. The area parameter describes a shape of a geographic area, but does not identify where the geographic area is located. The area parameter is deterministically combined with the location identity attribute to yield the encryption key. The appliance that receives the encrypted digital information can generate a decryption key to decrypt the digital information based on the received area parameter and the appliance location determined in accordance with any of the

foregoing methods. If the appliance location is not within the proximate area of the location identity attribute, the appliance will be unable to generate a decryption key to decrypt the digital information. Thus, allowing decryption of the digital information only at the specific geographic location enforces the location identity.

In another specific embodiment of the invention based on the foregoing general embodiment, the location identity attribute is integrated with the digital information in a portion of a file containing the digital information. A software application or operating system that accesses the file would enforce the location identity by allowing access to the file only at the specific geographic location defined by the location identity attribute.

In yet another specific embodiment of the invention based on the foregoing general embodiment, the location identity attribute is enforced by a hardware controller associated with hardware element of an appliance, such as a hard disk controller or video controller. The digital information could only be retrieved from memory, or displayed on a video monitor, if the hardware element is located at the specific geographic location defined by the location identity attribute.

A more complete understanding of the system and method for using location identity to control access to digital information will be afforded to those skilled in the art, as well as a realization of additional advantages and objects thereof, by a consideration of the following detailed description of the preferred embodiment. Reference will be made to the appended sheets of drawings, which will first be described briefly.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic drawing illustrating access to digital information determined by location identity in accordance with an embodiment of the present invention;

Fig. 2 is a block diagram illustrating components of a location identity attribute;

Fig. 3 is a block diagram illustrating components of a location value of the location identity attribute;

Fig. 4 is a flowchart illustrating a method for associating a location identity attribute with digital information;

Fig. 5 is a flowchart illustrating a method for enforcing access to geolocked digital information using the location identity attribute;

Figs. 6A-6D are flowcharts illustrating alternative methods for determining location identity for an appliance;

Fig. 7 is a flowchart illustrating an encryption method for associating a location identity attribute with digital information;

Fig. 8 is a flowchart illustrating an encryption method for enforcing access to geolocked digital information using the location identity attribute;

Fig. 9 is a flowchart illustrating a file method for associating a location identity attribute with digital information;

Fig. 10 is a flow chart illustrating a file method for enforcing access to geolocked digital information using the location identity attribute;

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention satisfies the need for a way to control the interchange of digital information that allows control over security and access to the information, and which prevents unauthorized copying of copyright-protected content. In the detailed description that follows, like element numerals are used to describe like elements illustrated in one or more of the figures. Various terms are used throughout the detailed description, including the following:

Appliance. Electronic devices, systems, networks, and the like with the minimum capacity to acquire digital information, transmit the information, and acquire location information. These electronic devices will often include a processing capability to execute program instructions and a memory capacity for short term and long term data storage.

Associating Location Identity. The method of marking digital information with a location identity attribute.

Digital Information. Digital information is information that is represented in digital format. Examples of information that can be represented digitally include text, data, software, music, video, graphics, etc.

Enforcing Location Identity. The method of providing or denying access to digital information through its associated location identity attribute.

Geocode. A unique coding of a location on earth usually associated with a coordinate system. Some geocodes identify a point location, such as when a place is identified by its latitude and longitude. Other geocodes may identify a region such as a zip code.

Geolock. An enforced association between digital information and a geographic area defined by a location identity attribute.

Geolocked Information. Digital information that has been associated with a location identity attribute, and that can only be accessed within an area defined by the location identity attribute.

Location. Any geographic place. It may be, but is not limited to, a precise point location, an area or region location, a point location included within a proximate area, or combinations of places on earth. Location can also include height (or altitude) to identify position above or below the surface of the earth, or time to identify position in a temporal dimension.

Location Identity. A precise coding of a location. It can be used, but is not limited to, an attribute of information to precisely define the location at which the information is to be accessed. Location identity may be a coding of a point location, a region, a region with an associated point location, a corridor (i.e., center line with length on either side of the center line), or by any other precise identification of a location in space and time.

Location Variance. The minimum resolution at which a geocode of a location may fail to exactly distinguish it from adjacent locations. For example, if a military grid reference system is used with two characters of precision, then any location is precise to within only ten kilometers.

Playback Location. A location at which playback of digital information will be allowed.

Proximity. The zone or area that includes the location.

The foregoing definitions are not intended to limit the scope of the present invention, but rather are intended to clarify terms that are used in describing the present invention. It should be appreciated that the defined terms may also have other meanings to persons having ordinary skill in the art. These and other terms are used in the detailed description below.

Referring now to Fig. 1, a schematic illustration of the present invention depicts access to digital information determined by location identity. Location identity refers to an attribute of information that precisely determines the geographic area or region in which the information is accessible. Two geographic areas denoted by A and B are shown on a map 101 within the continental United States. Information 130 is represented in digital format, and has an associated location identity attribute 131 which precisely defines the geographic area A as the region in which the digital information can be accessed. If an appliance 112 is located within the geographic region A, then the digital information 130 will be accessible by the appliance. Conversely, if an appliance 122 is located within the geographic region B (or anywhere else besides geographic region A), then the digital information 130 will not be accessible. Location identity thus represents an attribute of digital information that determines the precise geographic region within which the information can be accessed. Digital information that have location identity are termed "geolocked" and systems that enforce location identity geolock the associated digital information to the geographic region defined by the location identity attribute.

Fig. 2 depicts a location identity attribute 140 as comprising two items of information: a location value 142, and a proximity value 143. The location value 142 corresponds to the unique position of a particular place. Many different coordinate systems, such as latitude and longitude, have been developed that provide unique numerical identification of any location. For the purposes of this invention, any coordinate system that uniquely identifies a place can be used for the location value 142 of the location identity attribute 140. The proximity value 143 corresponds to the extent of a zone or area that encompasses the location. The location identity attribute 140

may comprise a point location or an exact location if the proximity value 143 is set to zero, null, empty, etc., or some other value indicating that the area referred to by the location identity attribute is a unique point location. It should be appreciated that the proximity value 143 is different from location variance. The proximity value 143 refers to a representation of an area or region, whereas location variance is the minimum resolution at which a geocode or a location may fail to exactly distinguish it from an adjacent location.

Fig. 3 depicts the location value 142 in greater detail. As noted above, there are numerous different coordinate systems in common use that provide a set of numbers that uniquely identify every location within the coordinate system. In the present invention, the location value 142 is defined in terms of a unique location designation or geocode as shown at 142a. Latitude 144 and longitude 145 using a conventional coordinate system may then further define the geocode. Other known systems, such as the Earth Centered, Earth Fixed Cartesian coordinate system, Universal Transverse Mercator (UTM), Military Grid Reference System (MGRS), World Geographic Reference System (GEOREF) etc., could also be advantageously utilized. In addition to latitude 144 and longitude 145, the location value could further include an altitude 146 as shown at 142b, which corresponds to the height of the location above sea level. Alternatively, the location value could further include a time value 147 that may be defined in terms of a date and/or time range. This allows the definition of location identity to consider both geographic and/or temporal access to information.

Any geographic region or area that contains the location value 142 of the location identity can serve as the proximity value 143 for the location identity attribute 140. The proximity value 143 may comprise a rectangular region defined by two adjacent longitude lines (providing horizontal edges) and two adjacent latitude lines (providing vertical edges). Alternatively, the proximity value 143 may comprise a circular region represented by a single number defining the radius around the location. The circular region can be further defined as an elliptical area either centered at the location, or a circular or elliptical area that contains the location but not necessarily as the centroid. In

another alternative, the proximity value 143 may comprise an irregular closed polygon, or a corridor. In yet another alternative, the proximity value 143 may correspond to a known geographic region, such as the country of Brazil. Other types of known geographic regions that can define the proximity value 143 can include postal zip codes, states, counties, incorporated cities, etc.

In accordance with the invention, whenever digital information is saved, stored, or copied, a location identity attribute 140 is associated with the digital information so that subsequent access of the digital information is limited to the geographic area specified by the location identity attribute 140. Fig. 4 illustrates a general method for associating digital information with the location identity attribute 140 that precisely defines the region in which access or playback of the digital information will be allowed. It should be appreciated that this method is analogous to the setting of a file attribute, such as a read-only attribute, for a computer file when the file is saved. The method would be performed by a system or device having a data processing capability and memory sufficient to generate, handle or process digital information for communication or distribution to another party, such as a personal computer, server, personal digital assistant (PDA), laptop, workstation, network, and the like. Software or embedded firmware instructions operating on the system or device would cause the method to be performed.

More particularly, the method starts at step 200 with a command to save or store digital information with a location identity attribute. At step 202, a location value 142 for the digital information is retrieved and stored for later use. The location value 142 is not necessarily the geographical location at which the method is invoked on the appliance, but rather corresponds to the location identity attribute (described above) for an appliance at which access to the digital information will be allowed. At step 204, a proximity value 143 of the location identity attribute of the appliance is retrieved and stored for later use. Various methods for generating the location and proximity values 142, 143 will be described in greater detail below. In addition to such methods, the location and proximity values 142, 143 may also be pre-stored and retrieved from

memory, or the end user may be queried to provide the information. At step 206, the retrieved location and proximity values 142, 143 are used to generate the location identity attribute 140. Then, at step 210, the digital information 216 is associated with the location identity attribute 140 to provide geolocked digital information 218.

Attempts to access geolocked information through a read or copy operation performed by a playback appliance will be denied unless the appliance confirms a valid location identity. This is performed by evaluating the associated location identity of the digital information against the location of the playback appliance to determine whether there is a match. Fig. 5 shows a general method for enforcing access to digital information by location identity. Logically, this method is analogous to the way that operating systems currently enforce a read-only attribute on files, i.e., allowing the user to access the file for reading, but denying access for writing. The method would be performed by a system or device having a data processing capability and memory sufficient to enable receipt of digital information communicated or distributed by another party, such as a personal computer, server, router, personal digital assistant (PDA), workstation, network, laptop, and the like. Software or embedded firmware instructions operating on the system or device would cause the method to be performed.

Particularly, the method starts at step 220 with a command to access the digital information. At step 222, the geolocked digital information 218 is accessed to read and store the associated location identity attribute 140. It should be appreciated that only the location identity portion of the geolocked information is accessed, and not the digital information itself. The location identity 140 of the geolocked information is stored for further use in the method. At step 224, the method determines the location of the appliance accessing the digital information. As will be described below, there are numerous possible ways to determine the appliance location 160. The appliance location 160 is stored for further use in the method. At step 226, the method determines whether the location of the appliance is consistent with the region defined by the location identity 140. If the appliance location 160 is consistent with the location identity 140, then access to the geolocked digital information 218 is allowed at step 228.

Conversely, if the appliance location 160 is not consistent with the location identity 140, then access is denied at step 230.

Figs. 6A-6D illustrate a plurality of exemplary methods to determine the playback location of the appliance that seeks access to the geolocked digital information. These methods would be performed by a system as part of the process of enforcing location identity with digital information, as described above with respect to Fig. 4. It should be appreciated that other methods for determining the playback location of the appliance could also be advantageously utilized.

Fig. 6A shows an address decoding method 240 in which a geocode is resolved from the street address for the appliance that will receive the geolocked digital information. At step 242, the address for the appliance is retrieved. The address information may be recalled from memory based on a previous communication with the appliance in which the address was obtained. Alternatively, the appliance may prompt to provide the address information as an initial part of an information transaction. Once the address information is retrieved, the address information is decoded to derive a specific geocode at step 244. This step may utilize a commercially available software program that can generate a coordinate specific geocode from an address, such as the MapMarker OCX Component Version 4.2 from the MapInfo Corporation located in Troy, New York. If it is desired to include a time element with the location identity attribute, then at step 246 the current time would be retrieved from the appliance, such as by reading the time from the appliance system clock. It should be appreciated that this step 246 is optional, and in many applications a time element would not be required. Lastly, at step 248, the geocode and time are converted to a format usable as the location value 142 for the location identity attribute 140.

Fig. 6B shows an appliance license method 250 in which the location value is derived from a license stored on the appliance. A license pack is a familiar feature of many systems and is generally used to validate access to application programs. License packs are digital files that contain information regarding the user/licensee. While not unbreakable, they are organized and encrypted in a way that makes them a

reliable way of validating the user. In this embodiment of the invention, the license pack would include a coordinate specific geocode identifying the location of the appliance. At step 252, the license pack stored on the appliance is accessed and retrieved. Then, a geocode is recovered from the license at step 254. If it is desired to include a time element with the location identity attribute, then at step 256 the current time would be retrieved from the appliance, such as by reading the time from the appliance system clock. It should be appreciated that this step 256 is optional, and in many applications a time element would not be required. Lastly, at step 258, the geocode and time are converted to a format usable as the location value 142 for the location identity attribute 140.

Fig. 6C shows a GPS data recovery method 260 in which the location value is recovered from a GPS receiver embedded in the appliance. As known in the art, the Global Positioning System (GPS) is a satellite-based radio-navigation system developed and operated by the U.S. Department of Defense. GPS permits land, sea, and airborne users to determine their three-dimensional position, velocity, and time, twenty-four hours a day in all weather, anywhere in the world. The GPS system provides civilian users with an accuracy of less than one hundred meters, while military users have an even greater degree of accuracy. The GPS position information is based on a system of coordinates called the World Geodetic System 1984 (WGS 84), and is similar to the latitude and longitude coordinate system. The commercial availability of GPS receivers is increasingly common, and in this embodiment it is anticipated that the appliance include an embedded GPS receiver. For example, GPS receivers are available as PCMCIA cards such as the NavCard made by the Rockwell Corporation or the GPScard from Trimble Navigation, and the Novatel Corporation makes a GPS receiver for a general purpose IBM PC. At step 262, the GPS receiver embedded in the appliance is accessed. A geocode is recovered from the embedded GPS receiver at step 264. Optionally, a time value may also be recovered from the GPS receiver. Lastly, at step 266, the geocode and optional time value are converted to a format usable as the location value 142 for the location identity attribute 140.

Fig. 6D shows a triangulation data recovery method 270 to determine the location of the appliance. As known in the art, triangulation is a method often employed by satellites, cellular phones, navigational systems, and other radio signal operators to provide accurate position information. The Loran-C System is an example of a commercially available navigation system that provides location information by triangulating RF signals from a plurality of fixed position RF transmitters. At step 272, the system will determine the direction to the appliance by accessing a RF signal communicated by the appliance. A geocode is calculated from the RF signal using a triangulation algorithm at step 274. Lastly, at step 276, the geocode is converted to a format usable as the location value 142 for the location identity attribute 140. If a time element is needed in the location identity attribute 140, then the current time would be read from the appliance system clock in the same manner as described above.

In accordance with an embodiment of the invention, the digital information is encrypted before transfer to an appliance and the location identity attribute 140 is used to generate a location identity based key used to encrypt the digital information. The layer of encryption added to the digital information enforces the limitation on access defined by the location identity attribute 140. Fig. 7 illustrates an encryption method for associating digital information with the location identity attribute 140. The method starts at step 300 with a command to save or store digital information with a location identity attribute. At step 302, a location value 142 for the digital information is retrieved and stored for later use. At step 304, a proximity value 143 of the location identity attribute of the appliance is retrieved and stored for later use. At step 306, the location and proximity values 142, 143 are used to generate an area parameter 190 that defines a shape of the geographic region defined by the location and proximity values, but which does not identify the location. The area parameter 190 may correspond to the proximity value 143. The location and proximity values 143 are used to generate a cryptographic location identity key 170 at step 308. Then, at step 310, the digital information 312 in cleartext form is deterministically combined with the location identity key 170 by an encryption algorithm to provide encrypted geolocked digital information 314 in ciphertext

form. This way, the cleartext would be encrypted based on the location identity key 170, such that the location identity attribute is cryptographically integrated with the digital information. The area parameter 190 would also be attached to the geolocked digital information 314 in cleartext form. It should be appreciated that other methods of generating the area parameter 190 may be utilized, as long as the area parameter alone is insufficient to generate the location identity key, but only when combined with the location of the appliance produces the location identity key.

Attempts to access the encrypted geolocked information through a read or copy operation performed by a playback appliance will be denied unless the appliance enforces the location identity. Fig. 8 shows a method for enforcing access to digital information by cryptographic location identity. The method starts at step 320 with a command to access the digital information. At step 322, the encrypted geolocked digital information 314 is accessed to recover the area parameter 190. It should be appreciated that at this point only the area parameter 190 is accessed, but not the encrypted geolocked information. At step 324, the method determines the location of the appliance accessing the digital information, such as using one of the methods described above. The appliance location 160 is stored for further use in the method. The method proceeds to step 328 in which the appliance location 160 is combined with the area parameter 190 to generate a cryptographic location identity key 170. It should be appreciated that the cryptographic location identity key 170 generated in step 328 will match the cryptographic location identity key generated previously in step 308 (see above) only if the appliance location 160 is within the region defined by the location identity attribute. The cryptographic location identity key 170 is then used in an encryption algorithm in step 330 to decrypt the geolocked digital information 314 and produce the cleartext digital information 312. It is noted that this method is not dependent upon any particular type of encryption algorithm and could be adapted for use with any known encryption method, including secret key encryption and public key encryption.

In another embodiment of the invention, the location identity attribute 140 is associated with a file containing digital information by an application or operating system of an appliance so that subsequent access of the digital information by the application or operating system is limited to the geographic area specified by the location identity attribute 140. Unlike the embodiment of Fig. 4 (described above) which was directed primarily to the communication of digital information between parties, this embodiment is most applicable to the management of data files by an application program or operating system executing on an individual appliance or a network of appliances. Particularly, this method is directed to the inclusion of a location identity attribute with a file (e.g., in the file header) which is used by an application program such as a word processing program, e-mail client or database manager to determine access to the file. It should be appreciated that an operating system could incorporate the present method into drivers that control basic system file operations, including save, store, copy, delete, and read commands. This is analogous to the way file attributes, such as read/write attributes, are handled in UNIX, Windows and VAX/DCL operating systems.

Fig. 9 illustrates a file method for associating digital information with the location identity attribute 140 that precisely defines the region in which access of a digital information file by an application or operating system will be allowed. The method starts at step 400 with a command to save or store a file containing digital information with a location identity attribute. This command may be performed as part of the ordinary operation of an application or operating system. At step 402, a location value 142 for the digital information is retrieved and stored for later use. At step 404, a proximity value 143 of the location identity attribute of the appliance is retrieved and stored for later use. As described above, various methods for generating the location and proximity values 142, 143 may be utilized. At step 406, the retrieved location and proximity values 142, 143 are used to generate the location identity attribute 140. Then, at step 408, the digital information 416 is integrated with the location identity attribute 140 to provide geolocked digital information 418. There are many ways in which to

integrate the digital information 416 with the associated location identity attribute 140. For digital information 416 stored as a file, the location identity can be formatted and appended to the front of the digital information file, such as in a header. Alternatively, the location identity attribute 140 can be saved in an associated directory file. In either case, an application or operating attempting to access the digital information file will enforce location identity by determining whether the location identity attribute 140 allows access to the geolocked digital information.

Attempts to access geolocked information through a read or copy operation performed by an application or operating system executing on the appliance will be denied unless the appliance complies with the location identity. Fig. 10 shows a file method for enforcing access to geolocked digital information by location identity. The method starts at step 420 with a command to access the geolocked digital information. At step 422, the geolocked digital information 218 is accessed to recover the associated location identity attribute 140. It should be appreciated that only the location identity portion of the geolocked information is accessed, and not the digital information itself. At step 424, the method determines the location of the appliance accessing the digital information. As described above, there are numerous possible ways to determine the appliance location 160. The appliance location 160 is stored for further use in the method. At step 426, the method determines whether the location of the appliance is consistent with the region defined by the location identity 140. If the appliance location 160 is consistent with the location identity 140, then the application or operating system can access the geolocked digital information 218 at step 428. Conversely, if the appliance location 160 is not consistent with the location identity 140, then access is denied at step 430. Since access to the geolocked digital information can only be achieved through an application or through the operating system, the application or operating system will be able to robustly enforce access to the geolocked digital information.

In yet another embodiment of the invention, the method for associating digital information with the location identity attribute 140 can be implemented in a hardware

controller for an appliance. Every hardware device for an appliance (e.g., hard disk, DVD/CD-ROM, floppy disk, video display, etc.), has a corresponding hardware controller that performs a limited set of functions with the device in response to specific commands from a software operating system. As in the preceding embodiments, digital information is saved in association with a corresponding location identity attribute. Any attempt to read the digital information through a device level command will be carried out by the device hardware controller with respect to the location of the playback appliance and the location identity stored on the device.

Specifically, the hardware controller may be adapted to execute some or all aspects of the aforementioned methods, including steps 202-210 of the general method described above with respect to Fig. 4, and steps 222-230 of the general method described above with respect to Fig. 5. For example, a hard disk controller for a personal computer may be coded to implement the foregoing method such that every digital information file that is stored in the hard disk has a location identity attribute stored therewith or as part of a file directory. The device hardware controller may further include an integrated GPS receiver that can provide the device hardware controller with location and temporal information. As before, attempts to access the stored file will be blocked by the hardware controller unless the appliance location matches the location identity attribute. Similarly, a video controller may be coded to block display of a file unless the appliance location matches the location identity attribute.

There are numerous applications and data formats in which the location identity attribute can be used to control access to digital information. A user can receive geolocked digital information in electronic form using any conventional method, including via telephone line, fiber optic, cable television, satellite broadcast, wireless or other media. A user may also physically receive custom generated geolocked digital information from a store or vendor in the form of magnetic or other encoded media, e.g., CD-ROM, diskette, videocassette or tape. Similarly, geolocked digital information can be communicated over a network including wide area networks such as the Internet,

local networks such as intranets, dial-up access between a personal and server computers, as an attachment to e-mail, or through a digital cell phone or other wireless device. Geolocked digital information can be stored on diskette, CD-ROM, tape, fixed or removable hard disk, DVD/CD-ROMs, flash memory/disks, EEPROMs, etc. The types of digital information that can be protected in this matter can include music files (e.g., MP3), software, literary works, commercial transaction files, text files, video/graphics, paging messages, cell phone conversation and commerce, and digital film, to name a few.

In an exemplary application of the present invention, the location identity attribute may be used to combat the problem of piracy and unauthorized use and copying of digital film. A customer would rent or buy digital video media (e.g., DVD) in a manner analogous to that when renting or purchasing film at a commercial video rental store. The location identity attribute is utilized at the time of purchase of the digital video media. Specifically, the location identity attribute corresponding to the customer's home address would be physically stored on a re-writable portion of the digital video media. The DVD player in the customer's home will be coded to enforce the location identity attribute in order to limit the playback of the digital video media to the particular geographic region and time period. Even if the media is copied, lost or stolen, it can only be viewed within its playback region and time span, and thus serves as a robust solution to the problems associated with unauthorized use of digital media.

In another exemplary application, a customer orders digital film or audio through a vendor's catalog. The catalog may be hardcopy or Internet-based, and the order may be placed via postal mail, telephone, facsimile transmission or Internet-based transaction. By whatever method the order is placed, the customer's order indicates the playback location. When the order is filled by the vendor, the location identity attribute associated with the customer is determined and used to generate an encryption key which is then used to encrypt the digital information file for the media. The purchased media is then custom encrypted for the order, copied to a format such as DVD or CD-ROM, and packaged with a viewer that is also customized for the location identity

attribute. Even if the entire contents of the purchased media are copied, the viewer and media, customized with the location identity attribute, prevent viewing except in the allowable region. In this exemplary application, the use of location identity and customized encryption and viewers provides a robust solution to the problem of piracy and unauthorized use and copying of digital media.

In another exemplary application of the invention, location identity is used to "narrowcast" information over public networks. Narrowcasting refers to the transmission of information to a limited audience (in contrast with broadcasting whereby information is transmitted to a large audience). Many types of information are useable only within a location context, e.g., local weather, traffic information, movie schedules, store information, etc. Applications that use such location-dependent information may be referred to as location-based applications. Location identity provides a way to use a broadcast type protocol to send information over a network that is identified by the location for which it is pertinent, e.g., local area for weather; store location for sale and advertising information, etc. Using the location of the client appliance, the client applications can utilize the location identity attached to the information to screen information selectively based on their current location. It can also provide a way to establish a unique location-based shared cryptographic key to maintain secure confidential communications for geographically limited narrowcast applications.

In another exemplary application of the present invention, location identity is used to enhance confidentiality and security for wireless network connectivity. Wireless networking is coming of age with the advent of networking equipment and protocols such as the "Bluetooth" technology that allows wireless portable or workstations to connect to a network. "Bluetooth" is an open standard for short-range transmission of digital voice and data between mobile devices (e.g., laptops, PDAs, cellular telephones) and desktop devices that supports point-to-point and multipoint applications. Since every wireless appliance communicating over the network will have a unique location, location identity can be utilized to establish a unique shared cryptographic key that can

be used to maintain secure confidential communications for wireless devices connecting over a public network.

In still another exemplary application of the present invention, location identity is used to enhance confidentiality and security for users of web applications. Internet "cookies" provide a way to allow web applications to maintain state between separate web pages, and are widely implemented by allowing the server to set and store name/value pairs on the user's computer. A server delivers a cookie to the user computer containing a unique state identifier that is established and shared by the client and server. Allowing the server to set and store information on a user's computer, however, has raised confidentiality and security concerns. The present invention provides a new way to enhance confidentiality and security by allowing the client application to generate the unique state identifier, which can be shared with the server, and used to maintain state for a web-based application.

In each of the foregoing embodiments and exemplary applications, there are at least four logical boundaries that exist between the application program that accesses geolocked digital information and the peripheral and network environment in which these applications operate. These boundaries include: (1) the data acquisition/appliance boundary; (2) the storage/appliance boundary; (3) the user interface/appliance boundary; and (4) the appliance/acquiring location boundary. The data acquisition/appliance boundary refers to the enforcement of location identity at the point of acquisition of digital information by an appliance, e.g., the appliance that cannot acquire the digital information from another source unless the location identity attribute is satisfied. The storage/appliance boundary refers to the enforcement of location identity at the point of storage of digital information by an appliance, e.g., the appliance cannot recall a stored file from memory unless the location identity attribute is satisfied. The user interface/appliance boundary refers to the enforcement of location identity at the point of presenting the information to the user, e.g., the user cannot view the digital information on the monitor of the appliance unless the location identity attribute is satisfied. The appliance/acquiring location boundary refers to the limitations upon

access to geolocked data by validating the appliance location, e.g., the user cannot view, store, retrieve or otherwise utilize the digital information in any manner unless the appliance location is acquired using an embedded GPS receiver. It should be appreciated that the relative security provided by any particular implementation of the present invention is related to the boundary at which access control is enforced.

Having thus described a preferred embodiment of a system and method for using location identity to control access to digital information, it should be apparent to those skilled in the art that certain advantages of the invention have been achieved. It should also be appreciated that various modifications, adaptations, and alternative embodiments thereof may be made within the scope and spirit of the present invention. The invention is further defined by the following claims.

CLAIMS

What is Claimed is:

1. A method for controlling access to digital information, comprising:

associating with said digital information a location identity attribute that defines at least a specific geographic location, wherein said digital information can be accessed only at said specific geographic location.

2. The method of Claim 1, wherein said associating step further comprises generating said location identity attribute to include at least a location value and a proximity value.

3. The method of Claim 2, wherein said location value corresponds to a location of an intended recipient appliance of said digital information.

4. The method of Claim 2, further comprising generating said location identity attribute to include a temporal value.

5. The method of Claim 2, wherein said location value further comprises a latitude and longitude dimension.

6. The method of Claim 5, wherein said location value further comprises an altitude dimension.

7. The method of Claim 3, wherein said proximity value corresponds to a zone that encompasses said location.

8. The method of Claim 7, further comprising selecting said zone from a group consisting of a rectangular region, a polygonal region, a circular region, and an elliptical region.

9. The method of Claim 7, further comprising selecting said zone from a known geographic region including at least one of a postal zip code, a state, a city, a county, a telephone area code, and a country.

10. The method of Claim 1, further comprising enforcing said location identity attribute by allowing access to said digital information only at said specific geographic location.

11. The method of Claim 10, wherein said enforcing step further comprises identifying location of an appliance through which access to said digital information is sought.

12. The method of Claim 11, wherein said enforcing step further comprises comparing said appliance location to said specific geographic location defined by said location identity attribute, and allowing access to said digital information only if said appliance location falls within said specific geographic location.

13. The method of Claim 11, wherein said location identifying step further comprises resolving said appliance location from a street address for said appliance.

14. The method of Claim 11, wherein said location identifying step further comprises retrieving said appliance location from a file stored within said appliance.

15. The method of Claim 11, wherein said location identifying step further comprises recovering said appliance location from a GPS receiver embedded in said appliance.

16. The method of Claim 11, wherein said location identifying step further comprises recovering said appliance location by triangulating RF signals received by said appliance.

17. The method of Claim 1, wherein said associating step further comprises encrypting said digital information using an encryption key based at least in part on said location identity attribute.

18. The method of Claim 17, wherein said generating step further comprises generating an area parameter defining a region that encompasses said specific geographic location, and deterministically combining said area parameter with said location identity attribute to yield said encryption key.

19. The method of Claim 17, further comprising enforcing said location identity attribute by allowing decryption of said digital information only at said specific geographic location.

20. The method of Claim 19, wherein said enforcing step further comprises generating a decryption key based at least in part on said specific geographic location, said decryption key being thereby used to decrypt said digital information.

21. The method of Claim 1, wherein said associating step further comprises integrating said location identity attribute with said digital information.

22. The method of Claim 21, further comprising including said location identity attribute in a portion of a file containing said digital information.

23. The method of Claim 22, further comprising enforcing said location identity attribute by allowing access to said file by a corresponding software application only at said specific geographic location.

24. The method of Claim 1, further comprising enforcing said location identity attribute by allowing retrieval of said digital information from memory only at said specific geographic location.

25. The method of Claim 1, further comprising enforcing said location identity attribute by allowing visual display of said digital information only at said specific geographic location.

26. The method of Claim 1, further comprising storing said digital information and said location identity attribute in a fixed format including at least one of CD-ROM, DVD, diskette, videocassette, and tape.

27. The method of Claim 1, further comprising transmitting said digital information and said location identity attribute in electronic form via at least one of telephone line, video cable, satellite broadcast, fiber optic, and wireless.

28. An apparatus for controlling access to digital information, comprising:

a processor having memory adapted to store software instructions operable to cause said processor to associate with said digital information a location identity attribute that defines at least a specific geographic location, wherein said digital information can be accessed only at said specific geographic location.

29. The apparatus of Claim 28, wherein said location identity attribute further comprises at least a location value and a proximity value.

30. The apparatus of Claim 29, wherein said location value corresponds to a location of an intended recipient appliance of said digital information.

31. The apparatus of Claim 29, wherein said location identity attribute further comprises a temporal value.

32. The apparatus of Claim 29, wherein said location value further comprises a latitude and longitude dimension.

33. The apparatus of Claim 32, wherein said location value further comprises an altitude dimension.

34. The apparatus of Claim 29, wherein said proximity value corresponds to a zone that encompasses said location.

35. The apparatus of Claim 34, wherein said zone further comprises at least one of a rectangular region, a polygonal region, a circular region, and an elliptical region.

36. The apparatus of Claim 34, wherein said zone further comprises a known geographic region including one of a postal zip code, a state, a city, a county, a telephone area code, and a country.

37. The apparatus of Claim 28, further comprising means for enforcing said location identity attribute by allowing access to said digital information only at said specific geographic location.

38. The apparatus of Claim 37, wherein said enforcing means further comprises means for identifying location of an appliance through which access to said digital information is sought.

39. The apparatus of Claim 38, wherein said enforcing means further comprises means for comparing said appliance location to said specific geographic location defined by said location identity attribute, wherein access to said digital information is allowed only if said appliance location falls within said specific geographic location.

40. The apparatus of Claim 38, wherein said location identifying means further comprises means for resolving said appliance location from a street address for said appliance.

41. The apparatus of Claim 38, wherein said location identifying means further comprises means for retrieving said appliance location from a file stored within said appliance.

42. The apparatus of Claim 38, wherein said location identifying means further comprises means for recovering said appliance location from a GPS receiver embedded in said appliance.

43. The apparatus of Claim 38, wherein said location identifying means further comprises means for recovering said appliance location by triangulating RF signals received by said appliance.

44. The apparatus of Claim 28, wherein said memory further stores software instructions operable to cause said processor to encrypt said digital information using an encryption key based at least in part on said location identity attribute.

45. The apparatus of Claim 44, further comprising an area parameter defining a region that encompasses said specific geographic location, and said memory further stores software instructions operable to cause said processor to deterministically combine said area parameter with said location identity attribute to yield said encryption key.

46. The apparatus of Claim 44, further comprising means for enforcing said location identity attribute by allowing decryption of said digital information only at said specific geographic location.

47. The apparatus of Claim 46, wherein said enforcing means further comprises means for generating a decryption key based at least in part on said specific geographic location, said decryption key being thereby used to decrypt said digital information.

48. The apparatus of Claim 28, wherein said location identity attribute is integrated with said digital information.

49. The apparatus of Claim 48, wherein said location identity attribute is included in a portion of a file containing said digital information.

50. The apparatus of Claim 49, further comprising means for enforcing said location identity attribute by allowing access to said file by a corresponding software application only at said specific geographic location.

51. The apparatus of Claim 28, further comprising means for enforcing said location identity attribute by allowing retrieval of said digital information from memory only at said specific geographic location.

52. The apparatus of Claim 28, further comprising means for enforcing said location identity attribute by allowing visual display of said digital information only at said specific geographic location.

53. The apparatus of Claim 28, wherein said digital information and said location identity attribute are disposed in a fixed format including one of CD-ROM, DVD, diskette, videocassette, and tape.

54. The apparatus of Claim 28, wherein said digital information and said location identity attribute are transmitted in electronic form via one of telephone line, video cable, satellite broadcast, fiber optic, and wireless.

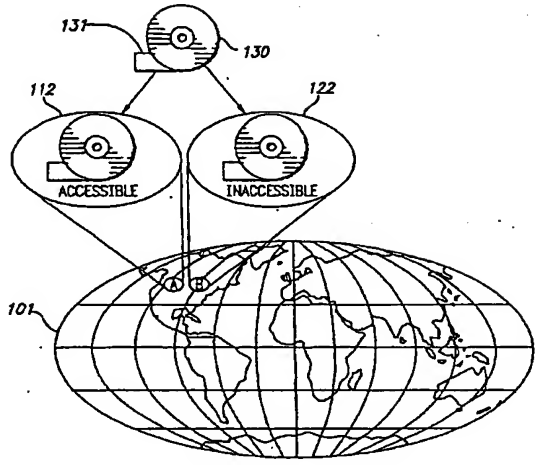

131
130
112
122
ACCESSIBLE
INACCESSIBLE
101

FIG. 1

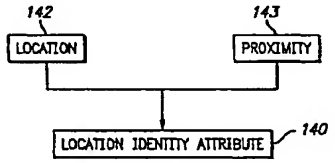

142
143
LOCATION
PROXIMITY
LOCATION IDENTITY ATTRIBUTE
140

FIG. 2

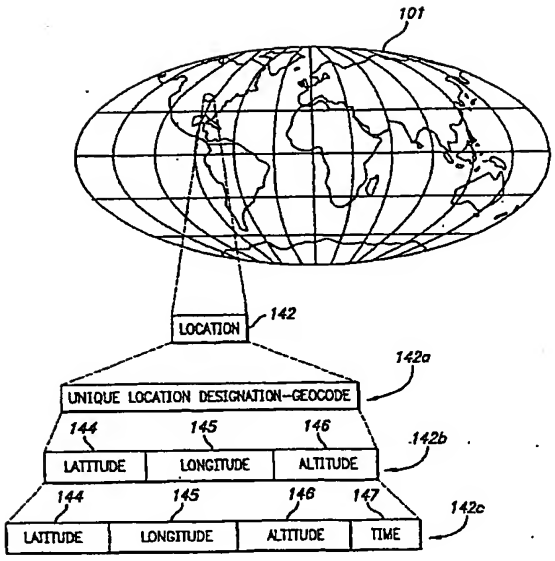

101
LOCATION
142
142a
UNIQUE LOCATION DESIGNATION-GEOCODE
144
145
146
142b
LATITUDE
LONGITUDE
ALTITUDE
144
145
146
147
142c
LATITUDE
LONGITUDE
ALTITUDE
TIME

FIG. 3

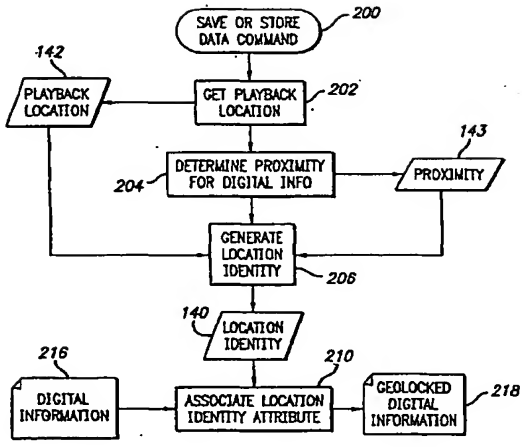

SAVE OR STORE DATA COMMAND
200
142
PLAYBACK LOCATION
GET PLAYBACK LOCATION
202
143
DETERMINE PROXIMITY FOR DIGITAL INFO
204
PROXIMITY
GENERATE LOCATION IDENTITY
206
140
LOCATION IDENTITY
216
210
DIGITAL INFORMATION
ASSOCIATE LOCATION IDENTITY ATTRIBUTE
GEOLOCKED DIGITAL INFORMATION
218

FIG. 4

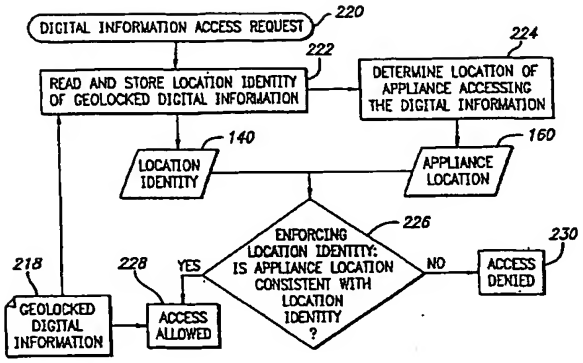

DIGITAL INFORMATION ACCESS REQUEST
220
READ AND STORE LOCATION IDENTITY OF GEOLOCKED DIGITAL INFORMATION
222
DETERMINE LOCATION OF APPLIANCE ACCESSING THE DIGITAL INFORMATION
224
LOCATION IDENTITY
140
APPLIANCE LOCATION
160
ENFORCING LOCATION IDENTITY: IS APPLIANCE LOCATION CONSISTENT WITH LOCATION IDENTITY ?
226
YES
NO
ACCESS DENIED
230
ACCESS ALLOWED
228
GEOLOCKED DIGITAL INFORMATION
218

FIG. 5

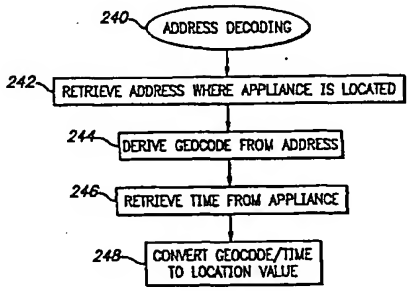

240
ADDRESS DECODING
242
RETRIEVE ADDRESS WHERE APPLIANCE IS LOCATED
244
DERIVE GEOCODE FROM ADDRESS
246
RETRIEVE TIME FROM APPLIANCE
248
CONVERT GEOCODE/TIME TO LOCATION VALUE

FIG. 6A

FIG. 6B

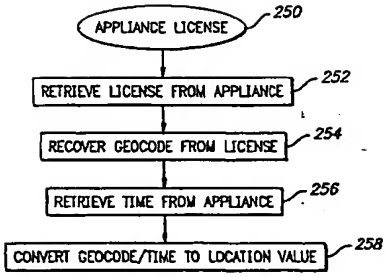


FIG. 6C

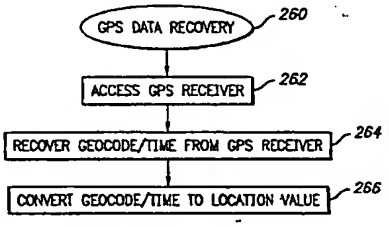
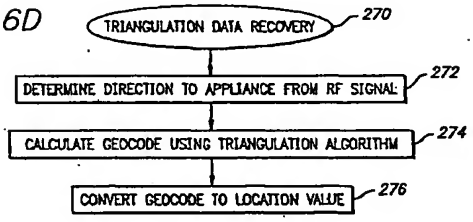


FIG. 6D



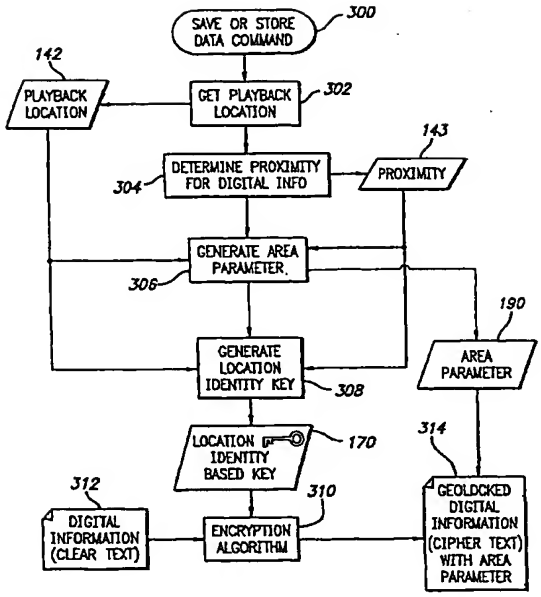

SAVE OR STORE DATA COMMAND
300
142
PLAYBACK LOCATION
GET PLAYBACK LOCATION
302
143
DETERMINE PROXIMITY FOR DIGITAL INFO
304
PROXIMITY
GENERATE AREA PARAMETER
306
190
GENERATE LOCATION IDENTITY KEY
308
AREA PARAMETER
LOCATION IDENTITY BASED KEY
170
314
312
DIGITAL INFORMATION (CLEAR TEXT)
ENCRYPTION ALGORITHM
310
GEOLOCKED DIGITAL INFORMATION (CIPHER TEXT) WITH AREA PARAMETER

FIG. 7

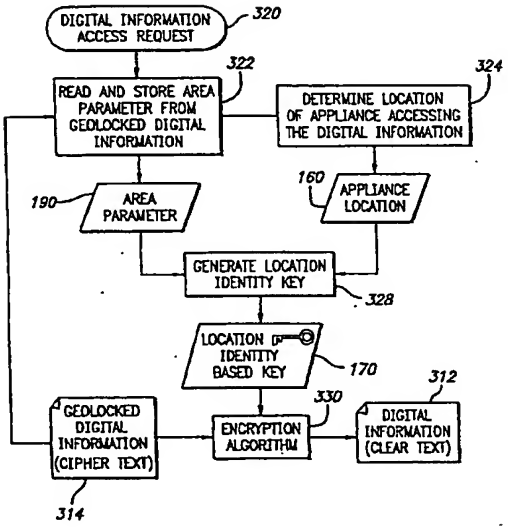

DIGITAL INFORMATION ACCESS REQUEST
320
READ AND STORE AREA PARAMETER FROM GEOLOCKED DIGITAL INFORMATION
322
DETERMINE LOCATION OF APPLIANCE ACCESSING THE DIGITAL INFORMATION
324
190
AREA PARAMETER
160
APPLIANCE LOCATION
GENERATE LOCATION IDENTITY KEY
328
LOCATION IDENTITY BASED KEY
170
330
312
GEOLOCKED DIGITAL INFORMATION (CIPHER TEXT)
ENCRYPTION ALGORITHM
DIGITAL INFORMATION (CLEAR TEXT)
314

FIG. 8

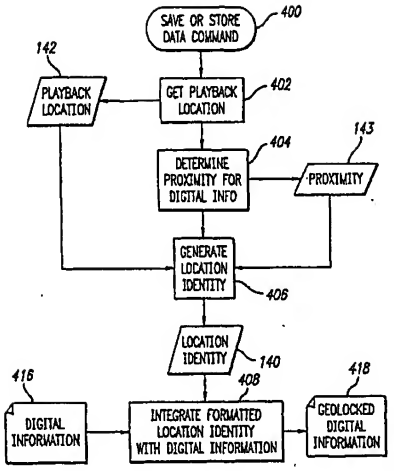

SAVE OR STORE DATA COMMAND
400
142
PLAYBACK LOCATION
GET PLAYBACK LOCATION
402
143
DETERMINE PROXIMITY FOR DIGITAL INFO
404
PROXIMITY
GENERATE LOCATION IDENTITY
406
LOCATION IDENTITY
140
416
408
418
DIGITAL INFORMATION
INTEGRATE FORMATTED LOCATION IDENTITY WITH DIGITAL INFORMATION
GEOLOCKED DIGITAL INFORMATION

FIG. 9

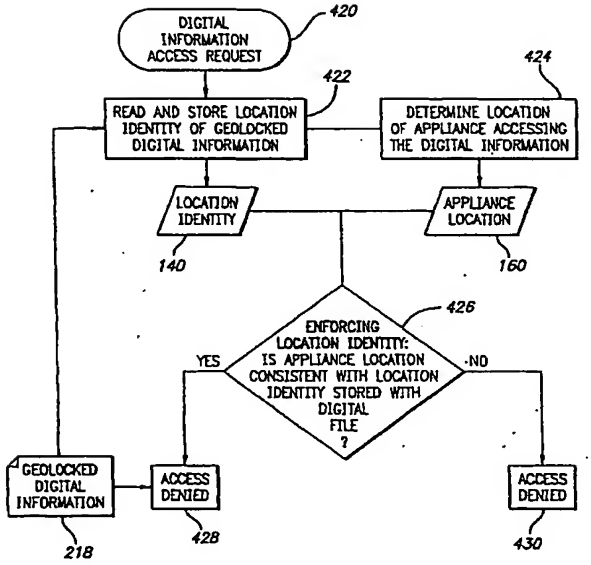

DIGITAL INFORMATION ACCESS REQUEST
420
READ AND STORE LOCATION IDENTITY OF GEOLOCKED DIGITAL INFORMATION
422
DETERMINE LOCATION OF APPLIANCE ACCESSING THE DIGITAL INFORMATION
424
LOCATION IDENTITY
140
APPLIANCE LOCATION
160
ENFORCING LOCATION IDENTITY: IS APPLIANCE LOCATION CONSISTENT WITH LOCATION IDENTITY STORED WITH DIGITAL FILE ?
426
YES
NO
GEOLOCKED DIGITAL INFORMATION
218
ACCESS DENIED
428
ACCESS DENIED
430

FIG. 10

【国際公開パンフレット（コレクトバージョン）】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 May 2002 (10.05.2002)

PCT

(10) International Publication Number
WO 02/037246 A3

(51) International Patent Classification⁷: G06F 1/00, G01S 5/14

(21) International Application Number: PCT/US01/48076

(22) International Filing Date: 30 October 2001 (30.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/699,832 30 October 2000 (30.10.2000) US

(71) Applicants and
(72) Inventors: SHLER, Mark [US/US]; 3480 Blair Drive, Los Angeles, CA 90068 (US). GLICK, Barry, J. [US/US]; 2710 Cathedral Avenue NW, Washington, DC 20008 (US). KARPF, Ronald, S. [US/US]; 11425 Brandy Hall Lane, Gaithersburg, MD 20878 (US).

(74) Agents: BERLINER, Brian, M. et al.; O'Melveny & Myers LLP, 400 South Hope Street, Los Angeles, CA 90071-2899 (US).

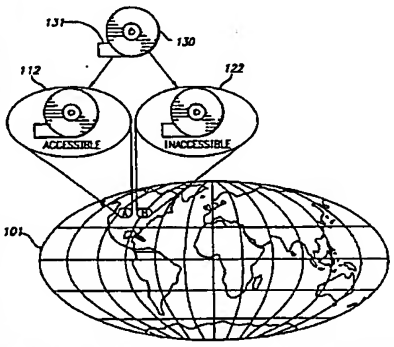
(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR USING LOCATION IDENTITY TO CONTROL ACCESS TO DIGITAL INFORMATION



(57) Abstract: A method and apparatus for controlling access to digital information utilizes a location identity attribute that defines a specific geographic location. The location identity attribute is associated with the digital information such that the digital information can be accessed only at the specific geographic location. The location identity attribute further includes a location value and a proximity value. The location value corresponds to a location of an intended recipient appliance of the digital information, and may be further defined in terms of latitude, longitude and altitude dimensions. The location identity attribute is enforced by allowing access to the digital information only at the specific geographic location. As a first part of this enforcement process, the location of an appliance through which access to the digital information is sought is identified. The appliance location is then compared to the specific geographic location defined by the location identity attribute, and access to the digital information is allowed only if the appliance location falls within the specific geographic location. There are many ways to identify the location of the appliance, including: (1) resolving the appliance location from a street address for the appliance; (2) retrieving the appliance location from a file stored within the appliance; (3) recovering the appliance location from a GPS receiver embedded in the appliance; and (4) recovering the appliance location by triangulating RF signals received by the appliance.

WO 02/037246 A3

WO 02/037246 A3

(88) Date of publication of the international search report:
9 October 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

【国際公開パンフレット（コレクトバージョン）】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 May 2002 (10.05.2002)

PCT

(10) International Publication Number
WO 02/037246 A3

(51) International Patent Classification⁷: G06F 1/00, G01S 5/14

(21) International Application Number: PCT/US01/48076

(22) International Filing Date: 30 October 2001 (30.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/699,832 30 October 2000 (30.10.2000) US

(71) Applicants and
(72) Inventors: SEILER, Mark [US/US]; 3480 Blair Drive, Los Angeles, CA 90068 (US). GLICK, Barry, J. [US/US]; 3710 Cathedral Avenue NW, Washington, DC 20008 (US). KARPF, Ronald, S. [US/US]; 11425 Brandy Hall Lane, Gaithersburg, MD 20878 (US).

(74) Agents: BERLINER, Brian, M. et al.; O'Melveny & Myers LLP, 400 South Hope Street, Los Angeles, CA 90071-2899 (US).

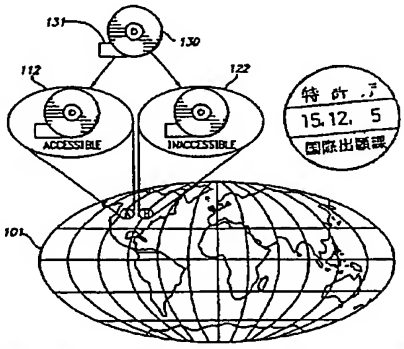
(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR USING LOCATION IDENTITY TO CONTROL ACCESS TO DIGITAL INFORMATION



(57) Abstract: A method and apparatus for controlling access to digital information utilizes a location identity attribute that defines a specific geographic location. The location identity attribute is associated with the digital information such that the digital information can be accessed only at the specific geographic location. The location identity attribute further includes a location value and a proximity value. The location value corresponds to a location of an intended recipient appliance of the digital information, and may be further defined in terms of latitude, longitude and altitude dimensions. The location identity attribute is enforced by allowing access to the digital information only at the specific geographic location. As a first part of this enforcement process, the location of an appliance through which access to the digital information is sought is identified. The appliance location is then compared to the specific geographic location defined by the location identity attribute, and access to the digital information is allowed only if the appliance location falls within the specific geographic location. There are many ways to identify the location of the appliance, including: (1) resolving the appliance location from a street address for the appliance; (2) retrieving the appliance location from a file stored within the appliance; (3) recovering the appliance location from a GPS receiver embedded in the appliance; and (4) recovering the appliance location by triangulating RF signals received by the appliance.

WO 02/037246 A3

2)

WO 02/037246 A3

(88) Date of publication of the international search report:
9 October 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/48076

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G01S5/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q G05F G08G G07C H04M H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, IBM-TDB, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	EP 0 997 808 A (DATUM INC) 3 May 2000 (2000-05-03) abstract paragraph '0001! paragraph '0004! page 2, line 21 - line 24 page 3, line 15 page 3, line 17 - line 18 paragraph '0023! —	1-16,26, 28-43,53 21-23, 48-50
X	US 6 046 689 A (NEWMAN BRYAN) 4 April 2000 (2000-04-04) column 4, line 27 -column 5, line 34 figure 1 abstract figure 2A —	1,27,28, 54

-/—

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 June 2003	05.08.03
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Chabot, P

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/48076

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 922 073 A (SHIMADA KAZUTOSHI) 13 July 1999 (1999-07-13) abstract column 2, line 1 - line 5 column 4, line 8 - line 17 figure 2	21-23, 48-50
A	US 6 057 779 A (BATES BENJAMIN G) 2 May 2000 (2000-05-02) abstract column 1, line 42 - line 46 column 1, line 61 -column 2, line 16	1-16, 28-43
A	WO 00 27143 A (SIGNALSOFT CORP) 11 May 2000 (2000-05-11) abstract page 3, line 16 - line 23 page 7, line 9 - line 22 page 7, line 30 - line 32	13-16, 40-43
X	US 4 418 425 A (FENNEL JR JOHN W ET AL) 29 November 1983 (1983-11-29) abstract figure 5 column 5, line 33 - line 40 column 5, line 52 - line 59	17-20, 44-47
X	US 5 640 452 A (MURPHY MICHAEL D) 17 June 1997 (1997-06-17) column 7, line 26 - line 29 column 7, line 52 - line 54 column 7, line 60 - line 65 column 8, line 49 - line 53 column 9, line 10 - line 13	25,52
X	WO 99 51038 A (PICCIONELLI GREG A ;RITTMASTER TED R (US)) 7 October 1999 (1999-10-07) page 3, line 18 - line 33 page 8, line 24 -page 9, line 5	24,51

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 01/48075

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet (1)) (July 1998)

International Application No. PCT/US 01 A8076

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-16,21-23,26-27,28-43,48-50,53-54

Digital information access control by associating with the information a geographic location attribute so as to make information only accessible in specific geographic locations. The location attribute is integrated with the digital information and the geographic location is retrieved via several methods.

2. Claims: 17-20,44-47

Digital information access control by associating with the information a geographic location attribute so as to make information only accessible in specific geographic locations. The digital information is encrypted with a key partially based in the geographic location.

3. Claims: 24,51

Digital information access control by associating with information a geographic location attribute so as to make information only accessible in specific geographic locations. Information location attribute is enforced by allowing retrieval in the specific geographic location.

4. Claims: 25,52

Digital information access control by associating with information a geographic location attribute so as to make information only accessible in specific geographic locations. Information location attribute is enforced by allowing information display in the specific geographic location.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US01/48076

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0997808	A	03-05-2000	US	6370629 B1	09-04-2002
			AU	5401599 A	04-05-2000
			BR	9904979 A	19-12-2000
			EP	0997808 A2	03-05-2000
			JP	2000163379 A	16-06-2000
			KR	2000035093 A	26-06-2000
			ZA	9906799 A	21-06-2000
US 6046689	A	04-04-2000	NONE		
US 5922073	A	13-07-1999	JP	9190236 A	22-07-1997
US 6057779	A	02-05-2000	NONE		
WO 0027143	A	11-05-2000	US	6321092 B1	20-11-2001
			AU	1339400 A	22-05-2000
			BR	9914975 A	02-04-2002
			CA	2349470 A1	11-05-2000
			EP	1133883 A1	19-09-2001
			WO	0027143 A1	11-05-2000
			US	2002077119 A1	20-06-2002
US 4418425	A	29-11-1983	DE	3261061 D1	29-11-1984
			EP	0073323 A1	09-03-1983
			JP	1060975 B	26-12-1989
			JP	1575114 C	20-08-1990
			JP	58043644 A	14-03-1983
US 6640452	A	17-06-1997	US	6317500 B1	13-11-2001
WO 9951038	A	07-10-1999	US	6154172 A	28-11-2000
			AU	3217299 A	18-10-1999
			CN	1330770 T	09-01-2002
			EP	1090307 A2	11-04-2001
			JP	2002510814 T	09-04-2002
			WO	9951038 A2	07-10-1999

Form PCT/ISA/210 (patent family annex) (July 1998)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NO,NZ,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TR,TT,TZ,UA,UG,US,UZ,VN,YU,ZA,ZW

(特許庁注：以下のものは登録商標)
ＵＮＩＸ
Ｗｉｎｄｏｗｓ
フロッピー

(74)代理人 100075672
弁理士 峰 隆司
(74)代理人 100109830
弁理士 福原 淑弘
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 シーラー、マーク
アメリカ合衆国、カリフォルニア州 ９００６８ ロサンゼルス、ブレアー・ドライブ ３４８０
(72)発明者 グリック、バリー・ジェイ
アメリカ合衆国、ワシントン・ディーシー ２０００８ カテドラル・アベニュー・エヌダブリュ ２７１０
(72)発明者 カーフ、ロナルド・エス
アメリカ合衆国、メリーランド州 ２０８７８ ゲイザースバーグ、ブランディ・ホール・レーン １１４２５
Ｆターム(参考) 5B017 AA06 CA16
5J104 AA12 PA14

【要約の続き】
ライアンス中に記憶されているファイルからのそのアプライアンス位置の検索、（３）アプライアンスに内蔵されたＧＰＳ受信機からのそのアプライアンス位置の復元、および（４）アプライアンスにより受信されたＲＦ信号を三角法で測定することによるアプライアンス位置の復元が含まれる。